明 細 書

不正機器検出装置、不正機器検出システム、不正機器検出方法、プログラム、記録媒体及び機器情報更新方法

技術分野

[0001] 本発明は、模倣により製造された不正な機器を検出する不正機器検出装置に関し、特に、映画や音楽などの著作物であるコンテンツを再生する再生装置の模倣機器を検出する技術に関する。

背景技術

[0002] 近年、DVDプレーヤー等のデジタルコンテンツを再生する再生装置に関し、正規な再生装置を不正にコピーしたクローン装置の存在が、重大な問題となっている。クローン装置は、正規な再生装置が保持しているデバイス鍵と同じ鍵を保持しており、著作権保護のため正規な再生装置にのみ復号再生を許可している暗号化コンテンツを、正規な再生装置が行うのと同じ方法で復号再生する。よって、前記クローン装置の所持者は、前記コンテンツを不正に視聴することが可能となる。

[0003] 上記問題に関連し、特許文献1には、正規な移動端末である携帯電話機について、クローン端末を検出する方法が開示されている。

特許文献1によると、クローン端末の検出装置は、同じ電話番号を持つ複数の移動端末が同時に複数の基地局の制御下に存在した場合に、クローン端末が存在すると判断する。

特許文献1:特開2000－184447号公報

発明の開示

発明が解決しようとする課題

[0004] しかしながら、前述の技術は、移動端末が基地局に対して位置登録を行うことを前提とするものであり、当該技術を、位置登録を行うことのないコンテンツ再生装置に係るシステムに適用することは、妥当でない。

上記問題に鑑み、本発明は、コンテンツの再生装置に係るクローン装置を検出することのできる、不正機器検出装置、コンテンツ再生装置、不正機器検出システム、情

報収集装置、不正機器検出方法、プログラム、記録媒体、機器情報更新方法及び集積回路を提供することを目的とする。

課題を解決するための手段

[0005] 上記課題を解決するために、本発明の不正機器検出装置は、模倣により製造された不正な機器を検出する不正機器検出装置であって、検証機器識別子と対応づけて保持している検証値とは異なる検証値を生成し、保持している前記検証値に替えて、生成した前記検証値と前記検証機器識別子とを対応づけて保持し、前記検証機器識別子を保持する機器に、生成した前記検証値を配布する配布手段と、不正検出の対象である検出対象機器により可搬媒体に書き込まれた対象機器識別子と検証値とを前記可搬媒体から取得する取得手段と、前記対象機器識別子と前記検証機器識別子とが一致する場合に、保持している検証値と取得した検証値とが一致するか否かを判定する判定手段と、一致しないと判定された場合に、前記対象機器識別子を不正機器リストに登録する登録手段とを備える。

発明の効果

[0006] 本発明の不正機器検出装置は、上述の構成を備えることにより、前記検証機器識別子と同じ対象機器識別子を保持している前記検出対象機器が、更新された検証値を保持しているか否かを判定するので、前記検証機器識別子を保持し更新前の検証値を保持する機器と、前記検証機器識別子を保持し更新後の検証値を保持する機器とが同時に存在するという状態を不正な状態として検知することができる。

[0007] ここで、前記登録手段による、検証値が一致しないと判定された対象機器識別子の不正機器リストへの登録とは、一致しないと判定された前記対象機器識別子を、他の対象機器識別子と区別して何らかの処理をするという概念を表している。

例えば、不正機器検出装置が、RAM上に複数の対象機器識別子を保持しており、一致しないと判定された前記対象機器識別子を他の対象機器識別子と区別して、別途設けたディスプレイ表示部に送信するというような場合も、一致しないと判定された前記対象機器識別子を不正機器リストに登録して、前記不正機器リストを前記表示部に送信していることとなる。前記不正機器リストは、最低限、RAMなどの揮発性メモリ上にあればよく、不揮発性メモリ等に保持する必要はない。

[0008] また、前記配布手段は、更に、前記判定手段により一致すると判定された場合に、保持している検証値とは異なる検証値を生成し、保持している前記検証値に替えて、生成した前記検証値と前記検証機器識別子とを対応づけて保持し、生成した前記検証値を前記検出対象機器に配布することとしてもよい。

この構成によれば、前記検証機器識別子と一致する前記検出対象機器の検証値を更新するので、新たな同一の検証値を、前記検出対象機器と前記不正機器検出装置とが保持することができる。

[0009] 再度、前記取得手段による対象機器識別子及び検証値の取得、前記判定手段による判定と同様の処理を行えば、前記検証対象識別子を保持しているにもかかわらず検証値の更新されない不正な検出対象機器を検出できる。

また、前記不正機器検出装置は、更に、暗号化コンテンツの復号のためのタイトル鍵を保持するタイトル鍵記憶手段を備え、前記配布手段は、更に、前記判定手段により一致すると判定された場合に、前記タイトル鍵を前記検出対象機器に配布することとしてもよい。

[0010] この構成によれば、前記コンテンツの復号、再生を、正規と判定された検出対象機器のみに許可することができるので、コンテンツが不当に再生されるのを防ぐことができる。

また、前記検出対象機器は、予め、個別鍵を保持しており、前記不正機器検出装置は、更に、暗号化コンテンツの復号のためのタイトル鍵を保持するタイトル鍵記憶手段と、前記検証機器識別子に対応づけて前記個別鍵の複製である複製鍵を保持している複製鍵記憶手段と、前記複製鍵を用いて前記タイトル鍵を暗号化する暗号化タイトル鍵生成手段とを備え、前記配布手段は、更に、前記判定手段により一致すると判定された場合に、暗号化された前記タイトル鍵を前記検出対象機器に配布することとしてもよい。

[0011] この構成によれば、前記タイトル鍵の復号を正規と判定された検出対象機器のみに許可することができるので、コンテンツが不当に再生されるのを防ぐことができる。

また、前記不正機器検出装置は、更に、過去に前記判定手段により一致すると判定された回数を計測する計測手段と、前記回数が所定回数を超えたか否かを判定

する回数判定手段とを備え、前記配布手段は、更に、前記回数が所定回数を超えた場合に、保持している検証値とは異なる検証値を生成し、保持している前記検証値に替えて、生成した前記検証値と前記検証機器識別子とを対応づけて保持し、生成した前記検証値を前記検出対象機器に配布することとしてもよい。

[0012] また、前記不正機器検出装置は、更に、前記配布手段により前記配布がされてから経過した期間を計測する計測手段と、経過した前記期間が、所定期間を超えたか否かを判定する期間判定手段とを備え、前記配布手段は、更に、前記期間が所定期間を超えたと判定された場合に、保持している検証値とは異なる検証値を生成し、保持している前記検証値に替えて、生成した前記検証値と前記検証機器識別子とを対応づけて保持し、生成した前記検証値を前記検出対象機器に配布することとしてもよい。

[0013] この構成によれば、新たな検証値の生成及び更新の回数を少なくすることにより、更新処理の負担を軽減することができる。

また、前記配布手段は、前記検証値として、乱数を生成することとしてもよい。

この構成によれば、検証が推測されることにより不正にコンテンツが再生される可能性を低減することができる。

[0014] 本発明のコンテンツ再生装置は、コンテンツの再生を行うコンテンツ再生装置であって、機器識別子と、模倣により製造された不正な機器を検出する不正機器検出装置により生成された検証値とを対応づけて記憶している記憶手段と、前記機器識別子と前記検証値とを、前記不正機器検出装置に通知する通知手段と、前記通知に対する応答として、前記不正機器検出装置により可搬媒体に書き込まれた、機器識別子と前記不正機器検出装置により生成された検証値とを、前記可搬媒体から取得する取得手段と、前記記憶手段に記憶されている前記機器識別子と取得した前記機器識別子とが一致する場合に、前記記憶手段に記憶されている検証値に替えて、取得した前記検証値と前記機器識別子とを対応づけて記憶させる更新手段とを備える。

[0015] この構成によれば、前記コンテンツ再生装置は、保持している検証値を不正機器検出装置により生成された検証値で書き換えるので、不正機器検出装置が生成した最

新の検証値を不正機器検出装置に通知することができ、古い検証値を通知することによって正規な機器であるにも関わらず、不正な機器であると誤判定されるのを防ぐことができる。

本発明の不正機器検出システムは、模倣により製造された不正な機器を検出する不正機器検出システムであって、不正機器検出装置と検出対象機器とから成り、前記検出対象機器は、対象機器識別子と検証値とを対応づけて記憶している記憶手段と、前記対象機器識別子と前記検証値とを前記不正機器検出装置に通知する通知手段と、前記不正機器検出装置により配布される、検証機器識別子と前記不正機器検出装置により生成された検証値とを取得する更新情報取得手段と、前記対象機器識別子と前記検証機器識別子とが一致する場合に、前記記憶手段に記憶されている検証値に替えて、取得した前記検証値と前記対象機器識別子とを対応づけて記憶させる更新手段とを含み、前記不正機器検出装置は、検証機器識別子と対応づけて保持している検証値とは異なる検証値を生成し、保持している前記検証値に替えて、生成した前記検証値と前記検証機器識別子とを対応づけて保持し、前記検証機器識別子を保持する機器に検証機器識別子と生成した前記検証値を配布する配布手段と、前記検出対象機器から、前記対象機器識別子と前記検証値とを取得する取得手段と、前記対象機器識別子と前記検証機器識別子とが一致する場合に、保持している前記検証値と取得した前記検証値とが一致するか否かを判定する判定手段と、一致しないと判定された場合に、前記対象機器識別子を不正機器リストに登録する登録手段とを含む。

[0016] この構成によれば、正規と判定された機器が保持する検証値は更新し、前記検証機器識別子と同じ対象機器識別子を保持している前記検出対象機器が、更新された検証値を保持しているか否かを判定するので、前記正規と判定された機器と、前記検証機器識別子を保持し更新前の検証値を保持する機器とが同時に存在するという不正な状態を検知することができる。

[0017] また、前記通知手段は、前記対象機器識別子と前記検証値とを可搬媒体に書き込み、前記取得手段は、情報収集装置を用いて、前記可搬媒体に記録された前記対象機器識別子と前記検証値とを読み出すこととしてもよい。

また、前記情報収集装置は、前記可搬媒体に書き込まれた対象機器識別子と検証値とを、当該可搬媒体から読み出す読出手段と、前記対象機器識別子と、前記検証値とを送信する送信手段とを含み、前記取得手段は、前記情報収集装置から前記対象機器識別子と前記検証値とを受信することとしてもよい。

[0018] この構成によれば、検出対象機器から可搬媒体を介して検証値を取得し、通信により不正機器検出装置に送信するので、複数の検出対象機器が地理的に散在している場合であっても、各検出対象機器が保持する検証値を前記不正機器検出装置に集約させることが出来る。

本発明の情報収集装置は、不正検出の対象である検出対象機器が保持する情報を、模倣により製造された不正な機器を検出する不正機器検出装置へ送信する情報収集装置であって、前記検出対象機器は、対象機器識別子と前記不正機器検出装置により生成された検証値とを保持しており、前記不正機器検出装置は、検証値を生成し、生成した検証値と検証機器識別子とを対応づけて保持し、対象機器識別子と検証値とを取得し、前記対象機器識別子と前記検証機器識別子とが一致する場合に、保持している検証値と取得した検証値とが一致するか否かを判定して一致しないと判定された場合に、前記対象機器識別子を不正機器リストに登録し、前記情報収集装置は、前記検出対象機器により可搬媒体に書き込まれた前記対象機器識別子と前記検証値とを、前記可搬媒体から読み出す読出手段と、読み出した前記対象機器識別子と前記検証値とを、前記不正機器検出装置に送信する送信手段とを備える。

[0019] この構成によれば、検出対象機器から可搬媒体を介して取得した検証値を、通信により不正機器検出装置に送信するので、複数の検出対象機器が地理的に散在している場合であっても、各検出対象機器が保持する検証値を前記不正機器検出装置に集約させることが出来る。

本発明の不正機器検出方法は、模倣により製造された不正な機器を検出する、記憶手段を備えた不正機器検出装置に用いられる不正機器検出方法であって、前記記憶手段に検証機器識別子と対応づけて保持している検証値とは異なる検証値を生成し、保持している前記検証値に替えて、生成した前記検証値と前記検証機器識

別子とを対応づけて前記記憶手段に保持させ、前記検証機器識別子を保持する機器に、生成した前記検証値を配布する配布ステップと、不正検出の対象である検出対象機器により可搬媒体に書き込まれた対象機器識別子と検証値とを前記可搬媒体から取得する取得ステップと、前記対象機器識別子と前記検証機器識別子とが一致する場合に、保持している検証値と取得した検証値とが一致するか否かを判定する判定ステップと、一致しないと判定された場合に、前記対象機器識別子を不正機器リストに登録する登録ステップとを含む。

[0020] 本発明のコンピュータプログラムは、模倣により製造された不正な機器を検出する、記憶手段を備えた不正機器検出装置に用いられるコンピュータプログラムであって、前記記憶手段に検証機器識別子と対応づけて保持している検証値とは異なる検証値を生成し、保持している前記検証値に替えて、生成した前記検証値と前記検証機器識別子とを対応づけて前記記憶手段に保持させ、前記検証機器識別子を保持する機器に、生成した前記検証値を配布する配布ステップと、不正検出の対象である検出対象機器により可搬媒体に書き込まれた対象機器識別子と検証値とを当該可搬媒体から取得する取得ステップと、前記対象機器識別子と前記検証機器識別子とが一致する場合に、保持している検証値と取得した検証値とが一致するか否かを判定する判定ステップと、一致しないと判定された場合に、前記対象機器識別子を不正機器リストに登録する登録ステップとを含む。

[0021] 本発明の記録媒体は、コンピュータ読み取り可能な記録媒体であって、前記コンピュータプログラムが記録されている。

この構成によれば、正規と判定された機器が保持する検証値は更新し、前記検証機器識別子と同じ対象機器識別子を保持している前記検出対象機器が、更新された検証値を保持しているか否かを判定するので、前記正規と判定された機器と、前記検証機器識別子を保持し更新前の検証値を保持する機器とが同時に存在するという状態を、不正な状態として検知することができる。

[0022] 本発明の機器情報更新方法は、コンテンツの再生を行うコンテンツ再生装置に用いられる機器情報更新方法であって、前記コンテンツ再生装置は、機器識別子と、模倣により製造された不正な機器を検出する不正機器検出装置により生成された検

証値とを対応づけて記憶する記憶手段を備え、前記機器情報更新方法は、前記機器識別子と前記検証値とを、前記不正機器検出装置に通知する通知ステップと、前記通知に対する応答として、前記不正機器検出装置により可搬媒体に書き込まれた、機器識別子と前記不正機器検出装置により生成された検証値とを、当該可搬媒体から取得する取得ステップと、前記記憶手段に記憶されている前記機器識別子と取得した機器識別子とが一致する場合に、前記記憶手段に記憶されている検証値に替えて、取得した前記検証値と前記機器識別子とを対応づけて記憶させる更新ステップとを含む。

[0023] 本発明のコンピュータプログラムは、コンテンツの再生を行うコンテンツ再生装置に用いられるコンピュータプログラムであって、前記コンテンツ再生装置は、機器識別子と、模倣により製造された不正な機器を検出する不正機器検出装置により生成された検証値とを対応づけて記憶する記憶手段を備え、前記コンピュータプログラムは、前記機器識別子と前記検証値とを、前記不正機器検出装置に通知する通知ステップと、前記通知に対する応答として、前記不正機器検出装置により可搬媒体に書き込まれた、機器識別子と前記不正機器検出装置により生成された検証値とを、当該可搬媒体から取得する取得ステップと、前記記憶手段に記憶されている前記機器識別子と取得した機器識別子とが一致する場合に、前記記憶手段に記憶されている検証値に替えて、取得した前記検証値と前記機器識別子とを対応づけて記憶させる更新ステップとを含む。

[0024] 本発明の記録媒体は、コンピュータ読み取り可能な記録媒体であって、前記コンピュータプログラムが記録されている。

本発明の集積回路は、コンテンツの再生を行うコンテンツ再生装置に用いられる集積回路であって、機器識別子と、模倣により製造された不正な機器を検出する不正機器検出装置により生成された検証値とを対応づけて記憶している記憶手段と、前記機器識別子と前記検証値とを、前記不正機器検出装置に通知する通知手段と、前記通知に対する応答として、前記不正機器検出装置により可搬媒体に書き込まれた、機器識別子と前記不正機器検出装置により生成された検証値とを、当該可搬媒体から取得する取得手段と、前記記憶手段に記憶されている前記機器識別子と取得

した前記機器識別子とが一致する場合に、前記記憶手段に記憶されている検証値に替えて、取得した前記検証値と前記機器識別子とを対応づけて記憶させる更新手段とを備える。

[0025] この構成によれば、前記コンテンツ再生装置が保持している検証値を不正機器検出装置により生成された検証値で書き換えるので、不正機器検出装置が生成した最新の検証値を不正機器検出装置に通知することができ、古い検証値を通知することによって正規な機器であるにも関わらず、不正な機器であると誤判定されるのを防ぐことができる。

図面の簡単な説明

[0026] [図1]本発明の実施の形態におけるクローン端末発見システムの構成を示す図である。

[図2]本発明の実施の形態における第1可搬媒体のデータ構造を示す図である。

[図3]本発明の実施の形態における第2可搬媒体のデータ構造を示す図である。

[図4]本発明の実施の形態における管理サーバの構成を示すブロック図である。

[図5]本発明の実施の形態における管理サーバの記録部に記録されるデータ構造を示す図である。

[図6]本発明の実施の形態における管理サーバの動作の一例を示すフローチャートである。

[図7]本発明の実施の形態における情報収集サーバの構成を示すブロック図である。

[図8]本発明の実施の形態における情報収集サーバの動作を示すフローチャートである。

[図9]本発明の実施の形態における利用者端末の構成を示すブロック図である。

[図10]本発明の実施の形態における利用者端末の記録部のデータ構造を示す図である。

[図11]本発明の実施の形態における利用者端末の第2可搬媒体を挿入した際の初期設定時、更新時動作を示すフローチャートである。

[図12]本発明の実施の形態における利用者端末のコンテンツ再生処理を示すフロー

チャートである。

符号の説明

[0027] 1 クローン端末発見システム

2 管理サーバ

3 情報収集サーバ

4 第1可搬媒体

5a～5m 第2可搬媒体

6a～6n 利用者端末

21 送受信部

22 表示部

23 記録部

24 制御部

31 送受信部

32 第2可搬媒体アクセス部

33 外部入力部

34 制御部

61 第2可搬媒体アクセス部

62 第1可搬媒体アクセス部

63 出力部

64 記録部

65 制御部

241 受信処理部

242 端末情報確認部

243 端末情報生成部

244 タイトル鍵暗号化部

245 送信データ生成部

246 送信処理部

341 第2可搬媒体挿入処理部

342 タイトル情報取得部

343 送信データ生成部

344 送信処理部

345 受信処理部

346 第2可搬媒体データ書込部

651 第2可搬媒体挿入処理部

652 端末情報書込部

653 暗号化タイトル鍵復号化部

654 端末情報更新部

655 第1可搬媒体挿入処理部

656 デスクランブル部

7 通信路

発明を実施するための最良の形態

[0028] 本発明の一実施形態に係るクローン端末発見システムは、製造業者により正規に製造されたDVDプレーヤー等の利用者端末が、不正な製造業者等により不正に複製されて市場に出回ってしまった場合に、その不正に複製された端末(以下、クローン端末という。)を発見するためのものである。

以下、前記クローン端末発見システムについて、図面を参照しながら説明する。

＜概要＞

本発明の一実施形態に係るクローン端末発見システム1は、図1に示すように、管理サーバ2と、情報収集サーバ3と、第1可搬媒体4と、m個(mは自然数)の第2可搬媒体5a～5mと、n台(nは自然数)の利用者端末6a～6nと、通信路7とから構成される。

[0029] 第1可搬媒体4は、タイトル鍵を用いて暗号化された動画コンテンツが記録されている光ディスク(例えばDVD－ROM)であり、小売店で販売される。

第2可搬媒体5a～5mは、データの書き換えが可能なポータブルメディア(例えばSDカード)であり、第1可搬媒体4に記録されている暗号化された動画コンテンツの復

号に必要な鍵や、クローン端末の発見に必要な、利用者端末に関する端末情報を保持し、利用者端末6a～6nと、情報収集サーバ3との間のデータのやりとりに用いられる。

[0030] 利用者端末6a～6nはそれぞれ、第1可搬媒体4に記録されている動画コンテンツの復号再生を行う再生装置（例えばDVDプレーヤー）であって、予め割り当てられた各端末に固有の個別鍵を保持しており、第2可搬媒体5a～5mのいずれかに記録されている情報と個別鍵とを用いて、暗号化された動画コンテンツのタイトル鍵を生成して、動画コンテンツを復号再生する。

[0031] 情報収集サーバ3は、第1可搬媒体4を販売する小売店に設置されたコンピュータ装置であり、第2可搬媒体5a～5mに記録されているデータの読み書きが可能であり、第2可搬媒体5a～5mのいずれかが挿入された場合に、挿入された第2可搬媒体から、当該第2可搬媒体に記録されている端末情報を読み出して、当該端末情報をネットワークである通信路7を介して接続する管理サーバ2へ送信し、応答として管理サーバ2から情報を受信して、受信した情報を挿入されている第2可搬媒体に書き込む。

[0032] 管理サーバ2は、クローン端末を発見するコンピュータ装置であり、通信路7を介して、情報収集サーバ3から利用者端末6a～6nの何れかに係る端末情報を受け取り、受けとった端末情報に係る利用者端末がクローン端末か否かを判定する。クローン端末でないと判定した場合には、前記動画コンテンツのタイトル鍵を暗号化した暗号化タイトル鍵と、端末情報に係る利用者端末が保持している端末情報を更新するための更新情報を生成して情報収集サーバ3に送信する。ここで、クローン端末は、正規の利用者端末の複製であり、複製元の利用者端末が保持しているのと同じ個別鍵を保持しているものとする。また、クローン端末か否かの判定に関しては、後に詳述する。

[0033] ここで、クローン端末を発見するまでの処理の流れについて、コンテンツの購入、再生を希望するユーザが、利用者端末6a、第2可搬媒体5aを所持してる場合を例に簡単に説明する。

前記ユーザは、先ず、自身が所有する第2可搬媒体5aを、自身が所有する利用者

端末6aに挿入する。利用者端末6aは、第2可搬媒体5aに、利用者端末6aの利用者端末識別子等の端末情報を書き込む。

[0034] 次に、ユーザは、第2可搬媒体5aを持参して小売店に行き、小売店に設置されている情報収集サーバ3に第2可搬媒体5aを挿入する。

情報収集サーバ3は、第2可搬媒体5aから端末情報を読み出して、管理サーバ2に送信する。

管理サーバ2においては、前記端末情報に基づき、前記端末情報に係る利用者端末がクローン端末か否かを判定し、クローン端末でない場合には、第1可搬媒体4に記録されている動画コンテンツの暗号化に用いたタイトル鍵を、前記端末情報に対応する利用者端末の個別鍵で暗号化することにより暗号化タイトル鍵を生成し、また、利用者端末6aが保持している端末情報を更新するための更新情報を生成し、暗号化タイトル鍵と更新情報とを情報収集サーバ3に送信する。

[0035] 情報収集サーバ3は、暗号化タイトル鍵と更新情報とを第2可搬媒体5aに書き込む。

前記ユーザは、第2可搬媒体5aと購入した第1可搬媒体4とを所持して帰宅し、第1可搬媒体4と第2可搬媒体5aとを利用者端末6aに挿入する。

利用者端末6aは、暗号化タイトル鍵を復号してタイトル鍵を生成し、第1可搬媒体4に記録されている暗号化された動画コンテンツを復号して再生し、また、更新情報に基づき、保持している端末情報を更新する。

＜構成＞

＜第1可搬媒体4の構成＞

第1可搬媒体4は、DVD－ROMであり、タイトル識別子と、当該タイトル識別子で識別されるコンテンツが暗号化された暗号化コンテンツとが記録されている。

[0036] タイトル識別子は、コンテンツの映画や曲のタイトル、シリアル番号（1、2、3、・・・）など第1可搬媒体4に蓄積されているコンテンツを一意に特定可能な識別子であり、コンテンツは、利用者端末6a～6nにおいて復号再生や外部出力が可能なMPEG2（Moving Picture Expert Group）フォーマットなどの形式で符号化されている。

[0037] 第1可搬媒体4は、一例として、図2に示すように、タイトル識別子401「TLID1」と、

暗号化コンテンツ402「ENCCNT1」を保持する。

ここで、ENCCNT1は、コンテンツ「CNT1」が、タイトル識別子「TLID1」に対応するタイトル鍵「TLK1」で暗号化されたものであり、Enc(TLK1、CNT1)と表す。Enc(K、P)の記載は、平文Pを暗号化鍵Kで暗号化した際の暗号文を示す。

[0038] なお、暗号、復号処理は、秘密鍵暗号方式によるものとし、本実施形態では一例として、ブロック暗号AESを用いるものとする。AESについては、公知であるので説明を省略する。

＜第2可搬媒体5aの構成＞

第2可搬媒体5aは、SDカードであり、利用者端末テーブルを保持する。

[0039] 前記利用者端末テーブルは、一以上の利用者端末情報から成り、利用者端末情報は、利用者端末識別子と、第1利用者端末乱数と、第2利用者端末乱数と、タイトル識別子と、暗号化タイトル鍵とから成る。

利用者端末識別子は、利用者端末6a～6nそれぞれを一意に識別するための識別子である。

[0040] 第1利用者端末乱数は、第2可搬媒体5aが前記利用者端末識別子により識別される利用者端末に最後に挿入された時点で当該利用者端末が保持していた乱数であり、当該利用者端末により書き込まれる。

第2利用者端末乱数は、利用者端末の保持する第1利用者端末乱数を更新するために、管理サーバ2によって生成された乱数であり、管理サーバ2から当該乱数を受信した情報収集サーバ3によって書き込まれる。

[0041] タイトル識別子は、第1可搬媒体4に記録されたコンテンツを一意に識別する識別子であり、情報収集サーバ3によって書き込まれる。

暗号化タイトル鍵は、前記タイトル識別子に対応するタイトル鍵が、前記利用者端末識別子により識別される利用者端末が保持する個別鍵を用いて暗号化されたものである。

ここで、第1利用者端末乱数と第2利用者端末乱数と個別鍵とタイトル鍵は、一例として128ビットの自然数であるとする。

[0042] また、第2利用者端末乱数の値が「0」である時は、利用者端末が保持している第1

利用者端末乱数の更新が不要であることを意味し、暗号化タイトル鍵の値が「0」であるときは、暗号化タイトル鍵が無効又は記録されていないことを意味する。

第2可搬媒体5aは、一例として図3(c)に示すように、利用者端末識別子511「TMIDa」と、第1利用者端末乱数512「TMRND1a」、第2利用者端末乱数「TMRND2a」、タイトル鍵「TLID1」、暗号化タイトル鍵「Enc(IKa, TLK1)」から成る利用者端末情報531を含む利用者端末テーブル501を保持する。

[0043] <管理サーバ2の構成>

管理サーバ2は、図4に示すように、送受信部21と表示部22と記録部23と制御部24とを含んで構成される。

管理サーバ2は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウス、モデムなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、管理サーバ2は、その機能を達成する。

[0044] 送受信部21は、モデム等であり、TCP/IP等の通信プロトコルを用い、通信路7を介して、情報収集サーバ3とデータの通信を行う。

表示部22は、液晶ディスプレイ等の表示装置であり、制御部24から表示指示を受信し、当該表示指示に基づき画面表示を行う。

記録部23は、図5に示すように、端末管理テーブル251と、タイトル管理テーブル252とを保持する。

[0045] 端末管理テーブル251は、複数の端末管理情報から成り、各端末管理情報は、利用者端末識別子と、第1管理サーバ乱数と、第2管理サーバ乱数と、個別鍵とから成る。

利用者端末識別子は、利用者端末6a～6nを識別する識別子である。

以下、利用者端末6x(xは、a～nのいずれかを示す)を識別する利用者端末識別子の値をTMIDxと示す。

[0046] 第2管理サーバ乱数は、利用者端末の保持する端末乱数を更新するために、後述する端末情報生成部243が生成した乱数であり、第1管理サーバ乱数は、端末情報

生成部243により1つ前に生成された乱数である。

第1管理サーバ乱数と第2管理サーバ乱数は、一例として128ビットの自然数であり、第2利用者端末乱数が「0」である場合は、第2利用者端末乱数が無効であることを示す。

[0047] 個別鍵は、利用者端末のそれぞれに付与されているユニークなデバイス鍵であり、利用者端末6aには、個別鍵IKaが付与されており、利用者端末6bには、個別鍵IKbが付与されており、以下同様に、利用者端末6nには、個別鍵IKnが付与されているものとする。

端末管理テーブル251は、一例として、図5に示すように、利用者端末6aを示す値TMIDaである利用者端末識別子262と、第1管理サーバ乱数263「CRND1a」と、第2管理サーバ乱数264「CRND2a」と、個別鍵265「IKa」とから成る端末管理情報261を含む。

[0048] 端末管理テーブル251には、正規の利用者端末が新たに製造されるごとに、新たな利用者端末に対応する端末管理情報が追記されるものとする。

タイトル管理テーブル252は、複数のタイトル管理情報から成り、各タイトル管理情報は、タイトル識別子と、タイトル鍵とから成る。

タイトル識別子は、コンテンツを識別する識別子であり、タイトル鍵は、前記タイトル識別子で識別されるコンテンツを暗号化及び復号するための鍵である。

[0049] また、タイトル管理テーブル252は、一例として、図5に示すように、タイトル識別子272「TLID1」と、TLID1で識別されるコンテンツのタイトル鍵であるタイトル鍵273「TLK1」とから成るタイトル識別情報271を含む。

タイトル管理テーブル252には、コンテンツ制作者により新たにコンテンツが生成されるごとに、新たなコンテンツに対応するタイトル管理情報が追記されるものとする。

[0050] 制御部24は、図4に示すように、受信処理部241と、端末情報確認部242と、端末情報生成部243と、タイトル鍵暗号化部244と、送信データ生成部245と、送信処理部246とを含んで構成される。制御部24は、各機能部を有する専用のマイクロコンピュータ等であり、各機能部は、マイクロコンピュータにマスクされているプログラムによって実現される。なお、各機能部は、独立のマイクロコンピュータであってもよい。

[0051] 受信処理部241は、情報収集サーバ3から送受信部21を介して、利用者端末識別子と第1利用者端末乱数とタイトル識別子を受け取る。そして、受け取った利用者端末識別子と第1利用者端末乱数を端末情報確認部242へ出力し、利用者端末識別子とタイトル識別子をタイトル鍵暗号化部244へ出力する。

端末情報確認部242は、受信処理部241から利用者端末識別子と第1利用者端末乱数を取得する。そして、受け取った利用者端末識別子に対応する第1管理サーバ乱数を記録部23から取得し、当該利用者端末識別子に対応する第2管理サーバ乱数が記録されている場合には、第2管理サーバ乱数も取得する。

[0052] まず、第2管理サーバ乱数が記録されている場合、第1利用者端末乱数と第2管理サーバ乱数が一致しているかどうか確認する。

そこで、第1利用者端末乱数と第2管理サーバ乱数が一致している場合、記録部23に記録されている第1管理サーバ乱数の値に第2管理サーバ乱数の値をコピーした後、第2管理サーバ乱数を消去する。そして、端末情報生成部243へ利用者端末識別子を出力し、タイトル鍵暗号化部244へ暗号化タイトル鍵生成要求を出力する。

[0053] 次に、第2管理サーバ乱数が記録されているが第1利用者端末乱数と第2管理サーバ乱数が一致しない場合、もしくは、第2管理サーバ乱数が記録されていない場合、第1利用者端末乱数と第1管理サーバ乱数が一致しているかどうか確認する。

第1利用者端末乱数と第1管理サーバ乱数が一致していない場合、利用者端末識別子に対応する利用者端末がクローンであることを示す画面を表示部22に表示させ、第1利用者端末乱数と第1管理サーバ乱数が一致していた場合、端末情報生成部243へ利用者端末識別子を出力し、タイトル鍵暗号化部244へ暗号化タイトル鍵生成要求を出力する。

[0054] 端末情報生成部243は、端末情報確認部242から利用者端末識別子を取得してまず乱数を生成し、当該乱数を記録部23に記録されている前記利用者端末識別子に対応する第2管理サーバ乱数に上書きするとともに、同一の乱数を、第2利用者端末乱数として送信データ生成部245へ出力する。ここで、端末情報生成部243は、少なくとも前回生成した乱数とは異なる乱数を生成するものとする。また、乱数を生成する方法については公知であるので説明を省略する。

[0055] タイトル鍵暗号化部244は、受信処理部241から利用者端末識別子とタイトル識別子を取得する。また、端末情報確認部242から暗号化タイトル鍵生成要求を取得する。そして、記録部23に記録されている端末管理テーブル251から、前記利用者端末識別子に対応する個別鍵を取得し、タイトル管理テーブル252から、前記タイトル識別子に対応するタイトル鍵を取得する。次に、タイトル鍵暗号化部244は、取得した個別鍵を基にタイトル鍵を暗号化して、暗号化タイトル鍵を生成し、取得した前記タイトル識別子と生成した前記暗号化タイトル鍵を送信データ生成部245へ出力する。

[0056] 送信データ生成部245は、端末情報生成部243から第2利用者端末乱数を取得する。また、タイトル鍵暗号化部244からタイトル識別子と暗号化タイトル鍵を取得する。そして、情報収集サーバ3へ送信するための、取得した第2利用者端末乱数とタイトル識別子と暗号化タイトル鍵を含む更新指示データを生成し、当該更新指示データを送信処理部246に出力する。

[0057] 送信処理部246は、送信データ生成部245から更新指示データを取得し、当該更新指示データを送受信部21を介して、情報収集サーバ3へ送信する。

＜情報収集サーバ3の構成＞

情報収集サーバ3は、図7に示すように、送受信部31と第2可搬媒体アクセス部32と外部入力部33と制御部34と表示部35から構成される。

[0058] 送受信部31は、モデム等であり、TCP／IP等の通信プロトコルを用い、通信路7を介して、管理サーバ2とデータの通信を行う。

第2可搬媒体アクセス部32は、SDカードリーダであり、情報収集サーバ3に設けられたSDカードスロット(図示せず)に第2可搬媒体が挿入されたことを検知した場合に制御部34に挿入通知を送信する。また、挿入された第2可搬媒体に記録されているデータの取得、及び挿入されている第2可搬媒体へのデータの記録を行う。

[0059] 外部入力部33は、数字0～9やアルファベットA～Zを入力可能なキーボードやキーパット、マウス等の、ユーザがタイトル識別子を入力するために用いる入力デバイスであり、入力されたタイトル識別子を、制御部34へと送信する。

本実施形態においては、前記入力されたタイトル識別子がTLID1であったものとする。

[0060] 表示部35は、液晶ディスプレイ等の表示装置であり、制御部34から表示指示を受信し、当該表示指示に基づき画面表示を行う。

制御部34は、第2可搬媒体挿入処理部341と、タイトル情報取得部342と、送信データ生成部343と、送信処理部344と、受信処理部345と、第2可搬媒体データ書込部346とを含む。

[0061] 制御部34は、各機能部を有する専用のマイクロコンピュータ等である。各機能部は、マイクロコンピュータにマスクされているプログラムによって実現される。なお、各機能部は、独立のマイクロコンピュータであってもよい。

第2可搬媒体挿入処理部341は、第2可搬媒体アクセス部32から前記挿入通知を取得した場合に、第2可搬媒体に記録されている利用者端末識別子と第1利用者端末乱数とを第2可搬媒体アクセス部32を介して取得する。

[0062] そして、取得した前記利用者端末識別子と前記第1利用者端末乱数とを送信データ生成部343へ出力し、タイトル情報要求をタイトル情報取得部342へ出力する。

タイトル情報取得部342は、第2可搬媒体挿入処理部341からタイトル情報要求を受け取った場合に、表示部35にタイトル識別子の入力を促すメッセージの表示指示を送信し、当該メッセージを表示させる。次に、ユーザが外部入力部33を用いて入力するタイトル識別子を取得し、取得した当該タイトル識別子を送信データ生成部343へ出力する。

[0063] 送信データ生成部343は、第2可搬媒体挿入処理部341から利用者端末識別子と第1利用者端末乱数を取得し、タイトル情報取得部342からタイトル識別子を取得する。

そして、管理サーバ2へ送信するための、取得した前記利用者端末識別子と前記第1利用者端末乱数と前記タイトル識別子とを含む送信データを生成し、その生成した送信データを送信処理部344に出力する。

[0064] 送信処理部344は、送信データ生成部343から前記送信データを取得し、取得した当該送信データを送受信部31を介して、管理サーバ2へ送信する。

受信処理部345は、送受信部31を介して管理サーバ2から、第2利用者端末乱数とタイトル識別子と暗号化タイトル鍵とを含む更新指示データを受け取り、更新指示

データに含まれる第2利用者端末乱数とタイトル識別子と暗号化タイトル鍵とを第2可搬媒体データ書込部346へ出力する。

[0065] 第2可搬媒体データ書込部346は、受信処理部345から第2利用者端末乱数とタイトル識別子と暗号化タイトル鍵を受け取り、受け取った第2利用者端末乱数とタイトル識別子と暗号化タイトル鍵とを第2可搬媒体アクセス部32を介して第2可搬媒体へ記録する。

＜利用者端末6aの構成＞

利用者端末6aは、図9に示すように、第2可搬媒体アクセス部61、第1可搬媒体アクセス部62、出力部63、記録部64、制御部65とから構成される。

[0066] 第2可搬媒体アクセス部61は、SDカードリーダであり、利用者端末6aに備えるカードスロット(図示せず)に第2可搬媒体が挿入されたことを検知し、挿入通知を制御部65に通知する。また、挿入されている第2可搬媒体からのデータの読み出し及び第2可搬媒体に対するデータの書き込みを行う。

第1可搬媒体アクセス部62は、DVDドライブであり、利用者端末6aが備えるディスクスロット(図示せず)に第1可搬媒体が挿入されたことを検知し、挿入通知を制御部65に通知する。また、第1可搬媒体アクセス部62は、挿入された第1可搬媒体からデータを読み出す。

[0067] 出力部63は、ディスプレイアダプタであり、液晶ディスプレイやプラズマテレビ等の外部ディスプレイと接続され、制御部65から受け取ったデータを当該外部ディスプレイに表示させる。

記録部64は、利用者端末識別子と、個別鍵と、端末保持乱数と、タイトル情報テーブルとを保持する。

[0068] 利用者端末識別子は、利用者端末を識別する識別子であり、当該利用者端末の出荷時に書き込まれる。

個別鍵は、利用者端末毎に異なる鍵であり、当該利用者端末の出荷時に書き込まれる。

端末保持乱数は、管理サーバ2によりクローン端末検出に用いられる乱数であり、利用者端末の出荷時には、初期値として値「0」が書き込まれる。

[0069] タイトル情報テーブルは、一以上のタイトル情報から構成され、タイトル情報は、タイトル識別子と、タイトル鍵とから成る。タイトル識別子は、コンテンツを識別する識別子であり、タイトル鍵は、タイトル識別子により識別されるコンテンツの暗号化及び復号に用いられる鍵である。

タイトル情報テーブルには、タイトル情報を新たに取得した場合に、当該タイトル情報を追記することができる。

[0070] 記録部64は、一例として図10に示すように、利用者端末識別子671「TMIDa」と、個別鍵672「IKa」と、端末保持乱数673「CRND1a」と、タイトル情報テーブル681とを保持しており、タイトル情報テーブル681は、値がTLID1であるタイトル識別子683と、TLID1で識別されるコンテンツの暗号化及び復号の鍵「TLK1」であるタイトル鍵684とから成るタイトル情報682を含む。

[0071] 制御部65は、第2可搬媒体挿入処理部651と、端末情報書込部652と、暗号化タイトル鍵復号化部653と、端末情報更新部654と、第1可搬媒体挿入処理部655と、デスクランブル処理部656とを含んで構成される。

制御部65は、各機能部を有する専用のマイクロコンピュータ等である。各機能部は、マイクロコンピュータにマスクされているプログラムによって実現される。なお、各機能部は、独立のマイクロコンピュータであってもよい。

[0072] 第2可搬媒体挿入処理部651は、第2可搬媒体アクセス部61から挿入通知を受信すると、記録部64に記録されている利用者端末識別子671「TMIDa」を取得する。

次に、第2可搬媒体アクセス部61経由で、第2可搬媒体に値が「TMIDa」である利用者端末識別子が記録されているか否かを確認し、第2可搬媒体に値が「TMIDa」である利用者端末識別子が記録されていない場合、端末情報書込部652へ利用者端末識別子671を出力し、処理を終了する。

[0073] 一方、第2可搬媒体に値が「TMIDa」である利用者端末識別子が記録されている場合には、第2可搬媒体に利用者端末識別子「TMIDa」に対応する第2利用者端末乱数とタイトル識別子と暗号化タイトル鍵が記録されているか否かを確認する。

ここで、第2可搬媒体に利用者端末識別子「TMIDa」に対応する第2利用者端末乱数が記録されている場合、読み出した第2利用者端末乱数を端末情報更新部65

4へ出力し、また、第2可搬媒体アクセス部61を介して、第2可搬媒体に記録されている第1利用者端末乱数を第2利用者端末乱数の値で上書きし、また、第2利用者端末乱数を消去する。

[0074] また、第2可搬媒体に利用者端末識別子「TMIDa」に対応するタイトル識別子と暗号化タイトル鍵が記録されている場合、タイトル識別子と暗号化タイトル鍵とを第2可搬媒体アクセス部61経由で第2可搬媒体から読み出して、読み出したタイトル識別子と暗号化タイトル鍵を暗号化タイトル鍵復号化部653へ出力するとともに、第2可搬媒体に記録されているタイトル識別子と暗号化タイトル鍵を消去する。

[0075] 暗号化タイトル鍵復号化部653は、第2可搬媒体挿入処理部651からタイトル識別子と暗号化タイトル鍵を取得し、記録部64から個別鍵IKaを取得する。

次に、個別鍵IKaを基に前記暗号化タイトル鍵の復号化を行うことによりタイトル鍵を取得し、前記タイトル識別子と当該タイトル鍵を記録部64のタイトル情報テーブル681に追記する。

[0076] 端末情報更新部654は、第2可搬媒体挿入処理部651から第2利用者端末乱数を取得し、記録部64に記録されている端末保持乱数の値を、取得した第2利用者端末乱数の値に変更する。

第1可搬媒体挿入処理部655は、第1可搬媒体アクセス部62から挿入通知を取得し、第1可搬媒体アクセス部62を介して、第1可搬媒体4に記録されているタイトル識別子を取得する。

[0077] そして、取得したタイトル識別子に対応するタイトル鍵が記録部64のタイトル情報テーブル681に記録されているか否かを判定し、記録されている場合、記録部64からタイトル鍵を取得し、取得したタイトル鍵をデスクランブル処理部656へ出力する。

デスクランブル処理部656は、第1可搬媒体挿入処理部655からタイトル鍵を取得し、第1可搬媒体アクセス部62経由で第1可搬媒体4に記録されている暗号化コンテンツを逐次取得し、前記タイトル鍵を基に暗号化コンテンツを逐次でスクランブルを行い、出力部63経由で外部へ逐次出力する。

[0078] 以上、利用者端末6aの構成について説明したが、他の利用者端末6b～6nについては、利用者端末識別子としてTMIDb～TMIDnをそれぞれ保持し、個別鍵としてI

Kb～IKnをそれぞれ保持している点が異なるのみであるので、説明を省略する。

＜動作＞

以下、クローン端末発見システム1の動作について、(1)初期設定、更新時動作、(2)コンテンツ購入時動作、(3)コンテンツ再生時動作の順に説明する。

[0079] ここで、(1)初期設定、更新時動作は、コンテンツの再生を行うユーザが、自身が所有する第2可搬媒体5aを、自身が所有する利用者端末6aに挿入したときの動作であり、(2)コンテンツ購入時動作は、前記ユーザが、第2可搬媒体5aを持参して小売店に行き、コンテンツが記録された第1可搬媒体4を購入し、小売店に設置されている情報収集サーバ3に第2可搬媒体5aを挿入したときの動作であり、(3)コンテンツ再生時動作は、前記ユーザが、第1可搬媒体4を購入して帰宅し、前記コンテンツを鑑賞するため、第1可搬媒体4と第2可搬媒体5aとを利用者端末6aに挿入したときの動作である。

[0080] (1)初期設定時、更新時動作

初期設定時動作、更新時動作について、図11を用いて説明する。

前提として、コンテンツの購入を希望するユーザは、利用者端末6a及び第2可搬媒体5aを所有しており、利用者端末6aの記録部64には、初期出荷時に、利用者端末識別子671として値TMIDaが書き込まれ、個別鍵672として値IKaが書き込まれ、第1利用者端末乱数673としてCRND1aが書き込まれており、第2可搬媒体5aの利用者端末テーブル501には、図3(a)に示すように何もデータが書き込まれていないものとする。

[0081] 前記ユーザは、先ず、第2可搬媒体5aを、利用者端末6aのカードスロットに挿入する。

第2可搬媒体アクセス部61は、挿入を検知し、第2可搬媒体挿入処理部651に対し挿入通知を送信する(ステップS601)。

第2可搬媒体挿入処理部651は、前記挿入通知を受け取ると、記録部64から利用者端末識別子671「TMIDa」を読み出す。(ステップS602)

第2可搬媒体挿入処理部651は、第2可搬媒体アクセス部61を介して、第2可搬媒体5a中のデータを検索し、「TMIDa」と同値の利用者端末識別子が記録されている

か否かを判定する(ステップS603)。

[0082] 第2可搬媒体5aに、値がTMIDaである利用者端末識別子が記録されていない場合(ステップS603:いいえ)、第2可搬媒体挿入処理部651は、端末情報書込部652へ利用者端末識別子TMIDaを出力し、端末情報書込部652は、第2可搬媒体挿入処理部651から利用者端末識別子TMIDaを取得する。

その後、端末情報書込部652は、記録部64から第1利用者端末乱数673「TMRND1a」を読み出し、利用者端末識別子671と第1利用者端末乱数673とを、第2可搬媒体アクセス部61を介して第2可搬媒体5aの利用者端末テーブル501に記録し、処理を終了する(ステップS604)。

[0083] このとき、第2可搬媒体5aに記録された利用者端末テーブル501は、図3(b)に示す状態となる。

一方、第2可搬媒体5aに、値がTMIDaである利用者端末識別子が記録されている場合(ステップS603:はい)、第2可搬媒体挿入処理部651は、第2可搬媒体5aに、利用者端末識別子「TMIDa」に対応する第2利用者端末乱数が記録されているか否かを判定し(ステップS605)、記録されていない場合(ステップS605:いいえ)、後述するステップS607に進む。

[0084] 利用者端末識別子「TMIDa」に対応する第2利用者端末乱数が記録されている場合(ステップS605:はい)、第2可搬媒体5aに記録された利用者端末テーブル501は、図3(c)に示す状態となっており、第2可搬媒体挿入処理部651は、第2利用者端末乱数TMRND2aを端末情報更新部654へ出力し、第2可搬媒体アクセス部61を介して、第2可搬媒体5aに記録されている第1利用者端末乱数を第2利用者端末乱数の値で上書きし、また、第2利用者端末乱数を消去する。

[0085] 端末情報更新部654は、第2可搬媒体挿入処理部651から第2利用者端末乱数TMRND2aを取得し、記録部64に記録されている端末保持乱数673の値を、第2利用者端末乱数TMRND2aの値で上書きする(ステップS606)。

次に、第2可搬媒体挿入処理部651は、第2可搬媒体アクセス部61を介して、第2可搬媒体5aに利用者端末識別子TMIDaに対応するタイトル識別子と、暗号化タイトル鍵が記録されているか否かを判定し(ステップS607)、記録されていない場合(ス

テップS607:いいえ)、処理を終了し、記録されている場合(ステップS607:はい)、前記タイトル識別子と、暗号化タイトル鍵とを読み出し、読み出した前記タイトル識別子と、暗号化タイトル鍵とを暗号化タイトル鍵復号化部653に送信し、第2可搬媒体アクセス部61を介して、第2可搬媒体5aに記録されている利用者端末識別子TMIDaに対応するタイトル識別子と、暗号化タイトル鍵とを消去する。

[0086] このとき、第2可搬媒体5aに記録された利用者端末テーブル501は、前述の図3(d)に示す状態となる。

暗号化タイトル鍵復号化部653は、第2可搬媒体挿入処理部651から前記タイトル識別子と前記暗号化タイトル鍵を取得し、記録部64から個別鍵672を取得し、当該個別鍵に基づき暗号化タイトル鍵の復号化を行い、タイトル鍵を取得する。

[0087] ここで、一例として、タイトル識別子が「TLID1」であり、前記暗号化タイトル鍵が、個別鍵「IKa」によりタイトル鍵「TLK1」が暗号化されたEnc(IKa, TLK1)であるとすると、暗号化タイトル鍵復号部653は、第2可搬媒体挿入処理部651からTLID1と、Enc(IKa, TLK1)とを取得し、記録部64から個別鍵672「IKa」を取得して、個別鍵IKaに基づき暗号化タイトル鍵Enc(IKa, TLK1)を復号し、タイトル鍵TLK1を取得することとなる。

[0088] 暗号化タイトル鍵復号化部653は、取得したタイトル識別子とそのタイトル鍵との組を、タイトル情報として記録部64に記録されているタイトル情報テーブル681に追記し(ステップS608)、処理を終了する。

(2)コンテンツ購入時処理

前述の(1)初期設定時動作により、第2可搬媒体5aには、利用者端末6aの端末情報である利用者端末識別子TMIDaと第1利用者端末乱数TMRND1aとが記録されているものとする。

[0089] 前記ユーザは、第2可搬媒体5aを持参して小売店に行き、タイトル識別子「TLID1」で識別されるコンテンツが暗号化されたENCCNT1(=ENC(TLK1, CNT1))が記録された第1可搬媒体4を購入し、前記ユーザは、情報収集サーバ3が備えるカードスロットに、第2可搬媒体5aを挿入する。

以下、コンテンツ購入時動作について、図8を用いて説明する。

[0090] 情報収集サーバ3において、第2可搬媒体アクセス部32は、前記カードスロットに第2可搬媒体5aが挿入されたことを検知し、挿入通知を第2可搬媒体挿入処理部341に送信する(ステップS301)。

第2可搬媒体挿入処理部341は、前記挿入通知を取得し、第2可搬媒体アクセス部32を介して、第2可搬媒体5aに記録されている利用者端末識別子TMIDaと第1利用者端末乱数TMRND1aを取得する(ステップS302)。

[0091] 第2可搬媒体挿入処理部341は、取得した利用者端末識別子TMIDaと第1利用者端末乱数TMRND1aを送信データ生成部343へ出力し、タイトル情報要求をタイトル情報取得部342へ出力する。(ステップS303)

タイトル情報取得部342は、第2可搬媒体挿入処理部341からタイトル情報要求を受け取り、表示部35にタイトル識別子の入力を促すメッセージの表示指示を送信し、表示部5は、前記表示指示に従って当該メッセージを表示する。

[0092] 前記ユーザは、前記メッセージに促され、外部入力部33を介して、購入したコンテンツを識別するタイトル識別子の値「TLID1」を入力する。

タイトル情報取得部342は、外部入力部33から、タイトル識別子TLID1を取得し(ステップS304)、取得したタイトル識別子を送信データ生成部343へ出力する(ステップS305)。

[0093] 送信データ生成部343は、第2可搬媒体挿入処理部341から利用者端末識別子TMIDaと第1利用者端末乱数TMRND1aを取得し、タイトル情報取得部342からタイトル識別子TLID1を取得し、取得した利用者端末識別子TMIDaと第1利用者端末乱数TMRND1aとタイトル識別子TLID1とを含む送信データを生成し、当該送信データを送信処理部344に出力する(ステップS306)。

[0094] 送信処理部344は、送信データ生成部343から前記送信データを取得し、取得した送信データを送受信部31を介して、管理サーバ2へ送信する(ステップS307)。

管理サーバ2は、前記送信データを受信して、当該送信データを用いて、後述するクローン判定処理を行う(ステップS308)。

管理サーバ2は、前記クローン判定処理において生成した端末更新データを、情報収集サーバ3に送信する

前記端末更新データには、第2利用者端末乱数TMRND2aとタイトル識別子TLID1と暗号化タイトル鍵ENCTLK1(=ENC(IKa, TLK1))が含まれる。

[0095] 情報収集サーバ3における、送受信部31は、通信路7を介して、管理サーバ2から前記端末更新データを受信するのを待ち(ステップS309:いいえ)、受信できた場合(ステップS309:はい)に、受信処理部345に当該端末更新データを送信する。

受信処理部345は、受信した端末更新データに含まれる第2利用者端末乱数TMRND2aとタイトル識別子TLID1と暗号化タイトル鍵ENCTLK1を第2可搬媒体データ書込部346へ出力する(ステップS310)。

[0096] 第2可搬媒体データ書込部346は、受信処理部345から第2利用者端末乱数TMRND2aとタイトル識別子TLID1と暗号化タイトル鍵ENCTLK1を受け取り、受け取った第2利用者端末乱数TMRND2aとタイトル識別子TLID1と暗号化タイトル鍵ENCTLK1を第2可搬媒体アクセス部32を介して、第2可搬媒体5aに記録する(ステップS311)。

[0097] ここで、前記ステップS308において、管理サーバ2により行われるクローン判定処理について、図6を用いて説明する。

管理サーバ2における送受信部21は、情報収集サーバ3から、前記送信データを受信し、当該送信データを、受信処理部241に送信する。

受信処理部241は、前記送信データを受信し、前記送信データに含まれる利用者端末識別子TMIDaと第1利用者端末乱数TMRND1aとを端末情報確認部242へ出力し、利用者端末識別子TMIDaとタイトル識別子TLID1をタイトル鍵暗号化部244へ出力する(ステップS201)。

[0098] 端末情報確認部242は、受信処理部241から利用者端末識別子TMIDaと第1利用者端末乱数TMRND1aを取得し(ステップS202)、記録部23に、利用者端末識別子TMIDaに対応する第2管理サーバ乱数CRND2aが記録されているか否かを判定し(ステップS203)、記録されていない場合(ステップS203:なし)、後述するステップS207に進み、記録されている場合(ステップS203:あり)、記録部23から第2管理サーバ乱数CRND2aを取得する(ステップS204)。

[0099] 端末情報確認部242は、第1利用者端末乱数TMRND1aの値と第2管理サーバ

乱数CRND2aの値が一致しているか否かを判定し(ステップS205)、一致していない場合(ステップS205:一致しない)、後述するステップS207に進み、一致している場合、利用者端末識別子TMIDaに対応する第1管理サーバ乱数CRND1aの値に第2管理サーバ乱数CRND2aの値をコピーし、第2管理サーバ乱数CRND2aを消去し、ステップS210に進む(ステップS206)。

[0100] 端末情報確認部242は、第1利用者端末乱数TMRND1aの値と第2管理サーバ乱数CRND2aの値が一致していると判定しなかった場合には(ステップS205:一致しない)、記録部23から、利用者端末識別子TMIDaに対応する第1管理サーバ乱数CRND1aを取得する(ステップS207)。

端末情報確認部242は、第1利用者端末乱数TMRND1aの値と第1管理サーバ乱数CRND1aの値を比較し(ステップS208)、一致していると判定した場合(ステップS208:はい)、ステップS210に進み、一致していない場合(ステップS208:いいえ)、利用者端末識別子TMIDaに対応する利用者端末がクローンであることを示す、例えば、「クローンを発見しました:利用者端末識別子TMIDa」と表示する画面を表示部22に表示させ(ステップS209)、ステップS210へ進む。

[0101] 端末情報確認部242は、端末情報生成部243へ利用者端末識別子TMIDaを出力し、タイトル鍵暗号化部244へ暗号化タイトル鍵生成要求を出力する(ステップS210)。

端末情報生成部243は、端末情報確認部242から利用者端末識別子TMIDaを取得して、新たに乱数を生成し、生成した乱数を記録部23の利用者端末識別子TMIDaに対応する第2管理サーバ乱数CRND2aの値として記録する。

また、前記乱数を、第2利用者端末乱数TMRND2aとして、送信データ生成部245へ出力する(ステップS211)。

[0102] タイトル鍵暗号化部244は、受信処理部241から利用者端末識別子TMIDaとタイトル識別子TLID1を取得し、端末情報確認部242から暗号化タイトル鍵生成要求を取得し、記録部23から、利用者端末識別子TMIDaに対応する個別鍵IKaと、タイトル識別子TLID1に対応するタイトル鍵TLK1を取得する。

そして、個別鍵IKaを基にタイトル鍵TLK1を暗号化して、暗号化タイトル鍵ENCT

LK1＝Enc(TLK1、IKa)を生成し、タイトル識別子TLID1と暗号化タイトル鍵ENCTLK1とを送信データ生成部245へ出力する(ステップS212)。

[0103] データ生成部245は、端末情報生成部243から第2利用者端末乱数TMRND2aを取得し、タイトル鍵暗号化部244からタイトル識別子TLID1と暗号化タイトル鍵ENCTLK1を取得する。

そして、取得した第2利用者端末乱数TMRND2aとタイトル識別子TLID1と暗号化タイトル鍵ENCTLK1とを含む端末更新データを生成し、当該端末更新データを送信処理部246に出力する(ステップS213)。

[0104] 送信処理部246は、送信データ生成部245から前記端末更新データを取得し、当該端末更新データを送受信部21を介して、情報収集サーバ3へ送信し、処理を終了する(ステップS214)。

(3)コンテンツ再生時処理

前記ユーザは、小売店で第1可搬媒体4を購入して帰宅し、前記コンテンツを鑑賞するため、第1可搬媒体4と第2可搬媒体5aとを利用者端末6aに挿入する。利用者端末6aに第2可搬媒体5aが挿入されると、利用者端末6aは、図11のステップS605～S608で示した更新処理を行う。

[0105] 以下、コンテンツ再生時処理について、図12を用いて説明する。

利用者端末6aが備えるディスクスロットに第1可搬媒体4が挿入された場合に、第1可搬媒体アクセス部62は、第1可搬媒体4の挿入を検知して、挿入通知を第1可搬媒体挿入処理部655に送信し、第1可搬媒体挿入処理部655が、前記挿入通知を受信する(ステップS651)。

[0106] 第1可搬媒体挿入処理部655は、第1可搬媒体アクセス部62を介して、第1可搬媒体4に記録されているタイトル識別子TLID1を取得する(ステップS652)。

第1可搬媒体挿入処理部655は、記録部64にタイトル識別子TLID1に対応するタイトル鍵TLK1が記録されているか否かを判定し(ステップS653)、記録されていない場合には(ステップS653:いいえ)、処理を終了し、記録されている場合には(ステップS653:はい)、第1可搬媒体4から読み出した前記タイトル識別子(TLID1)に対応する前記タイトル鍵(TLK1)を記録部64から読み出して(ステップS654)、当該タ

イトル鍵をデスクランブル処理部656へ出力する(ステップS655)。

[0107] デスクランブル処理部656は、第1可搬媒体挿入処理部655からタイトル鍵(TLK1)を取得し、その後、第1可搬媒体アクセス部62を介して第1可搬媒体4に記録されている暗号化コンテンツを逐次取得し、タイトル鍵TLK1を用いて読み出した暗号化コンテンツENCCNT1を逐次デスクランブルし、出力部63を介して外部ディスプレイに逐次出力する。

[0108] 読み出した暗号化コンテンツENCCNT1のデスクランブル及び外部への出力が終了した場合に、処理を終了する(ステップS656)。

<実施形態による効果についての補足説明>

本発明の実施形態の効果について、利用者端末の一つ(ここでは6aとする)が内部解析され、利用者端末6aの端末情報として利用者端末識別子TMIDaと個別鍵IKaと第1利用者端末乱数TMRND1aが外部へ漏洩した場合を例に挙げ、補足説明する。

[0109] まず、その利用者端末6aの端末情報が外部に漏洩した場合、その端末情報を保持する大量のクローン端末(ここではその一つを6yとする)が市場に出回る可能性がある。

つまり、利用者端末6aとクローン端末6yは同じ端末情報(利用者端末識別子TMIDaと個別鍵IKaと第1利用者端末乱数TMRND1a)を保持していることとなる。

ここでは、利用者端末6aの利用者(利用者aと呼ぶ)とクローン端末6yの利用者(利用者yと呼ぶ)は異なると想定し、また、利用者aと利用者yはそれぞれ異なる第2可搬媒体5aと第2可搬媒体5yを保持しているとする。

[0110] まず、一般的なシナリオとして、利用者端末6aの利用者aが小売店にコンテンツの入った第1可搬媒体4を購入しに行くとする。

その場合、利用者aの保持する第2可搬媒体5aを小売店に設置されている情報収集サーバ3に挿入する。

ここで、管理サーバ2は、第2可搬媒体5aに、暗号化されたタイトル鍵に加え、利用者端末識別子TMIDaの利用者端末向けの新たな乱数を第2利用者端末乱数として書き込む。

[0111] 利用者aはその第2可搬媒体5aを利用者端末6aに挿入し、利用者端末6aが保持する第1利用者端末乱数の値を第2可搬媒体5aに記録されている第2利用者端末乱数の値に更新する。

続いて利用者aが別のコンテンツを購入する際に、同様に第2可搬媒体5aを小売店に設置されている情報収集サーバ3に挿入する。

[0112] その際、第2可搬媒体5aには第1利用者端末乱数として新しい乱数の値が設定されている。

新しい乱数を、情報収集サーバ3を介して受け取った管理サーバ2は、利用者端末識別子TMIDaに対応する利用者端末6aの第1利用者端末乱数が更新されたことを認識する。

[0113] その後、クローン端末6yの利用者yがコンテンツを購入しに小売店に行くとする。

その際、利用者yは、同様に第2可搬媒体5yを小売店に設置されている情報収集サーバ3に挿入する。

その際、その利用者yが保持する第2可搬媒体5yには、利用者端末識別子TMIDaと、端末情報が漏洩した時点の古い第1利用者端末乱数が書き込まれている。

[0114] よって、管理サーバ2は、利用者端末識別子TMIDaに対応する利用者端末6xが、古い第1利用者端末乱数を保持していると認識する。

しかし、管理サーバ2は、利用者端末識別子TMIDaに対応する利用者端末6aの第1利用者端末乱数が新たな乱数に更新されたと認識している。

その結果から、同じ利用者端末識別子TMIDaを保持する利用者端末が市場に2台以上存在すると判断する。

[0115] そして、利用者端末識別子TMIDaに対応する利用者端末にクローンが存在する旨の警告を表示する。

このようにして、本発明の実施形態では、利用者端末のクローンが存在することを効率的に発見、検知することが出来る。

また、クローン利用者端末の別の形として、利用者端末の一つ(ここでも利用者端末6aとする)が内部解析され、利用者端末6aに関する端末情報(利用者端末識別子TMIDaと個別鍵とIKa第1利用者端末乱数TMRND1a)が外部へ漏洩した場合に

、クローン検知を逃れる目的で、その利用者端末識別子(TMIDa)を違う偽の値(ここではTMIDzとする)にしてクローン端末6zに埋め込む不正が考えられる。

[0116] しかし、本発明の実施形態では、管理サーバ2は購入した暗号化コンテンツのタイトル鍵を、受け取った利用者端末識別子に対応する個別鍵で暗号化した暗号化タイトル鍵を提供するようにした。

これにより、偽の利用者端末識別子TMIDzを管理サーバ2に渡した場合、そのクローン端末6zが保持する個別鍵IKaでは、受け取る暗号化タイトル鍵を復号化出来ないこととなる。

[0117] つまり、クローン端末6zでは購入したコンテンツの出力が出来ないこととなる。

これは、漏洩した利用者端末識別子を違う偽の値にして管理サーバ2へ提供しても意味がないことに繋がり、漏洩した利用者端末識別子を偽造することの抑止力として効果的である。

＜変形例＞

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において主な態様で実施し得るものである。以下のような場合も本発明に含まれる。

[0118] (1)本実施形態では、第2可搬媒体が情報収集サーバに挿入され、情報収集サーバから管理サーバ2が情報を取得する毎に、管理サーバ2は新たな乱数を生成し、それを第2利用者端末乱数として第2可搬媒体に記録するようにして、利用者端末の乱数を毎回更新するようにしていたが、これに限るものではない。例えば、ある一定期間(例えば一ヶ月)に一回のみ乱数を更新するようにしてもよい。また、外部から乱数更新要求信号を受けた時にのみ、乱数を更新するようにしてもよい。また、ある一定回数(例えば10回)コンテンツを購入する毎に、乱数を更新するようにしてもよい。これは、乱数を更新しない場合に、管理サーバ2は新たな乱数を生成せず、第2利用者端末乱数を第2可搬媒体に記録しないようにすることで実現可能である。

[0119] また、管理サーバ2に関し、ステップS205において一致しないと判定した後に、ステップS208において、第1利用者端末乱数TMRND1aの値と第1管理サーバ乱数CRND1aの値が一致していると判定した場合には、クローン端末ではないと決定し

ているが、これは、利用者端末6aにおいて、利用者端末6aの端末内部乱数が更新されるまでに、時間を要する場合があることを考慮してのものである。

[0120] 前記クローン端末の判定基準をより厳しくする場合には、ステップS205において一致しないと判定された場合に、クローン端末であるとみなして、ステップS209に進むこととすればよい。

(2)本実施形態においては、端末情報に乱数を用いていたが、該当端末を保持しない第三者ユーザによって推定できず、さらに、管理サーバ2が把握可能な値であれさえすれば、乱数でなくてもよい。例えば、シリアル番号で0から1つずつカウントアップしていってもよい。また、管理サーバ2が情報収集サーバ3からデータを受け取った時刻に関する情報でも良い。また、情報収集サーバ3へ第2可搬媒体が挿入された時刻に関する情報でも良い。また、情報収集サーバ3へ第2可搬媒体が挿入された延べ回数でも良い。また、対応する利用者端末で以前に外部へ出力したコンテンツタイトルの履歴に関する情報であってもよい。また、それらの値のハッシュ値であっても良い。

[0121] (3)本実施形態では、端末情報に乱数を用いていたが、該当端末を保持しない第三者ユーザによって推定できず、さらに、各利用者端末が自動で更新される値であれば、乱数でなくてもよい。例えば、利用者端末に第2可搬媒体が最後に挿入された時刻情報でも良い。また、利用者端末に第2可搬媒体が挿入された延べ回数でも良い。この場合、管理サーバ2は特に端末情報を更新する必要がなくなる。これにより、管理サーバ2の手間を軽減することが可能となる。

[0122] (4)本実施形態では、各ユーザが第2可搬媒体を一つずつ保持している場合を例に説明を行ったが、これに限られるものではない。たとえば、一人のユーザが二枚以上の第2可搬媒体を保持していても良い。このような場合に、同じ利用者端末識別子を複数の第2可搬媒体が保持し、管理サーバ2は、同じ利用者端末識別子を複数の第2可搬媒体経由で受け取る場合が考えられる。その際に、管理サーバ2は、その利用者端末識別子に対応する第2利用者端末乱数を、その内の一つの第2可搬媒体にのみ書き込んでも良いし、一つの利用者端末識別子に対応する同じ第2利用者端末乱数を、複数の第2可搬媒体に書き込むようにしても良い。前者の場合、第2利用

者端末乱数を書き込まれた第2可搬媒体をユーザが紛失した場合に、利用者端末の乱数を更新できないという欠点がある。一方、後者の場合、第2利用者端末乱数を書き込まれた第2可搬媒体をユーザが紛失した場合にでも、別の第2可搬媒体を用いて利用者端末の乱数を更新できるという利点がある。後者を実現するために、第2可搬媒体に記録する端末情報として乱数更新完了フラグを追加してもよい。乱数更新完了フラグは、第2可搬媒体に記録されている第2利用者端末乱数の値に、該当する利用者端末の第1利用者端末乱数の値の更新が完了した場合に、第2可搬媒体に書き込むフラグである。このようなフラグを追加することによって、一つの利用者端末識別子に対応する同じ第2利用者端末乱数を、複数の第2可搬媒体に書き込むようにして、その複数の第2可搬媒体を介して端末情報が管理サーバ2へ提供されたとしても、乱数更新完了フラグが記録されている場合にのみ利用者端末の乱数更新が完了したと認識することが出来る。

[0123] (5)本実施形態では、第2可搬媒体はSDカード等のポータブルメディアであったが、これに限るものではない。例えば、演算処理の可能なICカードでも良い。その場合、例えば、第2可搬媒体は、暗号処理等で利用者端末を認証してから端末情報やタイトル鍵情報を提供するようにしてもよい。これにより、より安全なシステムを構築することが出来る。また、変形例(4)の乱数更新完了フラグをICカード内で追加するようにしてもよい。これにより、不正な利用者端末が、第2可搬媒体に乱数更新完了フラグを立てないという不正を排除することが出来る。

[0124] また、第1可搬媒体4は、DVD－ROMとしたが、これに限らず、コンテンツの格納ができるBDや、CD－Rなどのメディアであってもよい。また、第2可搬媒体は、SDカードに限らず、データの書き換えが可能なポータブルメディアであればよい。

(6)本実施形態では、管理サーバ2は、第2可搬媒体経由での端末情報の収集に応答して、タイトル鍵情報を提供していたが、これに限るものはない。例えば、管理サーバ2は、第2可搬媒体経由で端末情報を収集するだけで、特に情報を提供しなくてもよい。また、管理サーバ2は、第2可搬媒体経由で端末情報を収集する見返りに一定期間(例えば1ヶ月)有効なライセンスを利用者端末に提供し、そのライセンスをある一定期間毎に取得しないと、利用者端末が利用不可になるような仕組みを備えて

いてもよい。

[0125] (7)本実施形態では、クローンを発見する対象は、コンテンツを出力する利用者端末であったが、本技術はこれに限るものではない。例えば、第2可搬媒体(例:SDカード)でも良い。また、電車の定期券や回数券や乗車券、ICカード、クレジットカード、キャッシュカード、デビットカード、電子マネー、電子チケット、電子パスポート(電子旅券)、入出門管理カード、運転免許書、住民基本台帳カード、携帯電話、PDA、STB(セットトップボックス)、電子ブック、コンピュータ、ICタグ、コンピュータソフトウエア、オンラインゲームのライセンスなどでもよい。この場合、クローンを発見する対象に、乱数を保持させることとなる。これにより、コンテンツを出力する利用者端末以外でも、クローンを発見することが出来る。

[0126] (8)本実施形態では、暗号化方法は、秘密鍵暗号方式AESを利用していたが、これに限るものではない。例えば、別の秘密鍵暗号方式(例えばDES)でも良いし、公開鍵暗号(例えばRSA方式)でもよいし、別の暗号方式でもよい。

(9)本実施形態では、管理サーバ2が、同一の利用者端末識別子に対応する異なる二種類の第1利用者端末乱数を受け取った場合に、その利用者端末識別子に対応する利用者端末はクローンであると判断していたが、これに限るものではない。例えば、同一の利用者端末識別子に対応するある閾値(例えば3)以上の異なる第1利用者端末乱数を受け取った場合に、その利用者端末識別子に対応する利用者端末はクローンであると判断してもよい。これにより、クローンの誤検知の確率を少なくすることが出来る。また、これは、同じ利用者端末識別子を複数の利用者端末が共有するようなシステムにも適用出来る。

[0127] 例えば、利用者端末識別子が、機種毎に共通な場合である。この場合、閾値としては、同じ利用者端末識別子を有する利用者端末の数以上に設定するようにする。このようにすることで、同じ利用者端末識別子を複数の利用者端末が共有するようなシステムであっても、クローンを検知することが出来る。

(10)管理サーバ2と、情報収集サーバ3とは、それぞれがモデム等を備えて、モデムを用いて通信することとしていたが、これには限らない。例えば、管理サーバ2の送受信部21及び情報収集サーバ3の送受信部31は、LANアダプタであって、通信路

7は、インターネットであってもよい。

[0128] (11)本実施形態では、13個の第2可搬媒体である第2可搬媒体5a～5mを用いた例で説明したが、これに限るものではない。例えば、12個以下でもよいし、14個以上であってもよい。また、14台の利用者端末である利用者端末6a～6nを用いた例で説明したが、これに限るものではない。例えば、15台以上であっても良いし、13台以下であっても良い。また、情報収集サーバ3の数は、1台以上であれば何台でも良い。また、第1可搬媒体4の数も、1個以上であれば何個でも良い。タイトル識別子及びタイトル鍵の種類も、1種類以上であれば何種類でも良い。

[0129] また、管理サーバ2が前記小売店に設置されるような場合は、情報収集サーバ3を用いずに、管理サーバ2と、第2可搬媒体であるSDカードのリーダライタ装置とを用いることとしてもよい。この場合、実施形態において情報収集サーバ3がユーザ入力により取得していたタイトル識別子は、管理サーバ2が取得すればよい。

(12)本実施形態では、小売店においてコンテンツを販売する場合を例に説明したが、これに限らず、本発明は、例えば、コンテンツをレンタルする場合や、リースする場合などにも適用可能である。

[0130] (13)管理サーバ2の制御部24、情報収集サーバ3の制御部34、利用者端末6a～6nの各制御部である制御部65における各機能ブロックは典型的には集積回路であるLSIとして実現されていてもよい。これらは個別に1チップ化されても良いし、一部又は全てを含むように1チップ化されても良い。

ここでは、LSIとしたが、集積度の違いにより、IC、システムLSI、スーパーLSI、ウルトラLSIと呼称されることもある。

[0131] また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセサで実現してもよい。LSI製造後に、プログラムすることが可能なFPGA(Field Programmable Gate Array)や、LSI内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサーを利用しても良い。

さらには、半導体技術の進歩又は派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

[0132] (14)本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしても良い。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD—ROM、MO、DVD、DVD－ROM、DVD－RAM、BD(Blu－ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

[0133] (15)上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

産業上の利用可能性

[0134] 本発明の不正機器検出装置、コンテンツ再生装置、情報収集装置、プログラム、記録媒体、集積回路は、著作権保護が必要なコンテンツの管理システムに用いられ、コンテンツの再生装置、当該再生装置の管理サーバなどデジタル家電機器、コンピュータ装置を扱う業者により、製造、販売等が成される。

請求の範囲

[1] 模倣により製造された不正な機器を検出する不正機器検出装置であって、

検証機器識別子と対応づけて保持している検証値とは異なる検証値を生成し、保持している前記検証値に替えて、生成した前記検証値と前記検証機器識別子とを対応づけて保持し、前記検証機器識別子を保持する機器に、生成した前記検証値を配布する配布手段と、

不正検出の対象である検出対象機器により可搬媒体に書き込まれた対象機器識別子と検証値とを前記可搬媒体から取得する取得手段と、

前記対象機器識別子と前記検証機器識別子とが一致する場合に、保持している検証値と取得した検証値とが一致するか否かを判定する判定手段と、

一致しないと判定された場合に、前記対象機器識別子を不正機器リストに登録する登録手段と

を備えることを特徴とする不正機器検出装置。

[2] 前記配布手段は、更に、前記判定手段により一致すると判定された場合に、保持している検証値とは異なる検証値を生成し、保持している前記検証値に替えて、生成した前記検証値と前記検証機器識別子とを対応づけて保持し、生成した前記検証値を前記検出対象機器に配布する

ことを特徴とする請求項1に記載の不正機器検出装置。

[3] 前記不正機器検出装置は、更に、

暗号化コンテンツの復号のためのタイトル鍵を保持するタイトル鍵記憶手段

を備え、

前記配布手段は、更に、前記判定手段により一致すると判定された場合に、前記タイトル鍵を前記検出対象機器に配布する

ことを特徴とする請求項2に記載の不正機器検出装置。

[4] 前記検出対象機器は、予め、個別鍵を保持しており、

前記不正機器検出装置は、更に、

暗号化コンテンツの復号のためのタイトル鍵を保持するタイトル鍵記憶手段と、

前記検証機器識別子に対応づけて前記個別鍵の複製である複製鍵を保持してい

る複製鍵記憶手段と、

前記複製鍵を用いて前記タイトル鍵を暗号化する暗号化タイトル鍵生成手段と

を備え、

前記配布手段は、更に、前記判定手段により一致すると判定された場合に、暗号化された前記タイトル鍵を前記検出対象機器に配布する

ことを特徴とする請求項2に記載の不正機器検出装置。

[5] 前記不正機器検出装置は、更に、

過去に前記判定手段により一致すると判定された回数を計測する計測手段と、

前記回数が所定回数を超えたか否かを判定する回数判定手段と

を備え、

前記配布手段は、更に、前記回数が所定回数を超えた場合に、保持している検証値とは異なる検証値を生成し、保持している前記検証値に替えて、生成した前記検証値と前記検証機器識別子とを対応づけて保持し、生成した前記検証値を前記検出対象機器に配布する

ことを特徴とする請求項1に記載の不正機器検出装置。

[6] 前記不正機器検出装置は、更に、

前記配布手段により前記配布がされてから経過した期間を計測する計測手段と、

経過した前記期間が、所定期間を超えたか否かを判定する期間判定手段と

を備え、

前記配布手段は、更に、前記期間が所定期間を超えたと判定された場合に、保持している検証値とは異なる検証値を生成し、保持している前記検証値に替えて、生成した前記検証値と前記検証機器識別子とを対応づけて保持し、生成した前記検証値を前記検出対象機器に配布する

ことを特徴とする請求項1に記載の不正機器検出装置。

[7] 前記配布手段は、前記検証値として、乱数を生成する

ことを特徴とする請求項1に記載の不正機器検出装置。

[8] コンテンツの再生を行うコンテンツ再生装置であって、

機器識別子と、模倣により製造された不正な機器を検出する不正機器検出装置に

より生成された検証値とを対応づけて記憶している記憶手段と、

前記機器識別子と前記検証値とを、前記不正機器検出装置に通知する通知手段と、

前記通知に対する応答として、前記不正機器検出装置により可搬媒体に書き込まれた、機器識別子と前記不正機器検出装置により生成された検証値とを、前記可搬媒体から取得する取得手段と、

前記記憶手段に記憶されている前記機器識別子と取得した前記機器識別子とが一致する場合に、前記記憶手段に記憶されている検証値に替えて、取得した前記検証値と前記機器識別子とを対応づけて記憶させる更新手段と

を備えることを特徴とするコンテンツ再生装置。

[9] 模倣により製造された不正な機器を検出する不正機器検出システムであって、不正機器検出装置と検出対象機器とから成り、

前記検出対象機器は、

対象機器識別子と検証値とを対応づけて記憶している記憶手段と、

前記対象機器識別子と前記検証値とを前記不正機器検出装置に通知する通知手段と、

前記不正機器検出装置により配布される、検証機器識別子と前記不正機器検出装置により生成された検証値とを取得する更新情報取得手段と、

前記対象機器識別子と前記検証機器識別子とが一致する場合に、前記記憶手段に記憶されている検証値に替えて、取得した前記検証値と前記対象機器識別子とを対応づけて記憶させる更新手段と

を含み、

前記不正機器検出装置は、

検証機器識別子と対応づけて保持している検証値とは異なる検証値を生成し、保持している前記検証値に替えて、生成した前記検証値と前記検証機器識別子とを対応づけて保持し、前記検証機器識別子を保持する機器に検証機器識別子と生成した前記検証値を配布する配布手段と、

前記検出対象機器から、前記対象機器識別子と前記検証値とを取得する取得手

段と、

前記対象機器識別子と前記検証機器識別子とが一致する場合に、保持している前記検証値と取得した前記検証値とが一致するか否かを判定する判定手段と、

一致しないと判定された場合に、前記対象機器識別子を不正機器リストに登録する登録手段と

を含むことを特徴とする不正機器検出システム。

[10] 前記通知手段は、前記対象機器識別子と前記検証値とを可搬媒体に書き込み、

前記取得手段は、情報収集装置を用いて、前記可搬媒体に記録された前記対象機器識別子と前記検証値とを読み出す

ことを特徴とする請求項9に記載の不正機器検出システム。

[11] 前記情報収集装置は、

前記可搬媒体に書き込まれた対象機器識別子と検証値とを、当該可搬媒体から読み出す読出手段と、

前記対象機器識別子と、前記検証値とを送信する送信手段と

を含み、

前記取得手段は、前記情報収集装置から前記対象機器識別子と前記検証値とを受信する

ことを特徴とする請求項10に記載の不正機器検出システム。

[12] 不正検出の対象である検出対象機器が保持する情報を、模倣により製造された不正な機器を検出する不正機器検出装置へ送信する情報収集装置であって、

前記検出対象機器は、対象機器識別子と前記不正機器検出装置により生成された検証値とを保持しており、

前記不正機器検出装置は、検証値を生成し、生成した検証値と検証機器識別子とを対応づけて保持し、対象機器識別子と検証値とを取得し、前記対象機器識別子と前記検証機器識別子とが一致する場合に、保持している検証値と取得した検証値とが一致するか否かを判定して一致しないと判定された場合に、前記対象機器識別子を不正機器リストに登録し、

前記情報収集装置は、

前記検出対象機器により可搬媒体に書き込まれた前記対象機器識別子と前記検証値とを、前記可搬媒体から読み出す読出手段と、

読み出した前記対象機器識別子と前記検証値とを、前記不正機器検出装置に送信する送信手段と

を備えることを特徴とする情報収集装置。

[13] 模倣により製造された不正な機器を検出する、記憶手段を備えた不正機器検出装置に用いられる不正機器検出方法であって、

前記記憶手段に検証機器識別子と対応づけて保持している検証値とは異なる検証値を生成し、保持している前記検証値に替えて、生成した前記検証値と前記検証機器識別子とを対応づけて前記記憶手段に保持させ、前記検証機器識別子を保持する機器に、生成した前記検証値を配布する配布ステップと、

不正検出の対象である検出対象機器により可搬媒体に書き込まれた対象機器識別子と検証値とを前記可搬媒体から取得する取得ステップと、

前記対象機器識別子と前記検証機器識別子とが一致する場合に、保持している検証値と取得した検証値とが一致するか否かを判定する判定ステップと、

一致しないと判定された場合に、前記対象機器識別子を不正機器リストに登録する登録ステップと

を含むことを特徴とする不正機器検出方法。

[14] 模倣により製造された不正な機器を検出する、記憶手段を備えた不正機器検出装置に用いられるコンピュータプログラムであって、

前記記憶手段に検証機器識別子と対応づけて保持している検証値とは異なる検証値を生成し、保持している前記検証値に替えて、生成した前記検証値と前記検証機器識別子とを対応づけて前記記憶手段に保持させ、前記検証機器識別子を保持する機器に、生成した前記検証値を配布する配布ステップと、

不正検出の対象である検出対象機器により可搬媒体に書き込まれた対象機器識別子と検証値とを当該可搬媒体から取得する取得ステップと、

前記対象機器識別子と前記検証機器識別子とが一致する場合に、保持している検証値と取得した検証値とが一致するか否かを判定する判定ステップと、

一致しないと判定された場合に、前記対象機器識別子を不正機器リストに登録する登録ステップと

を含むことを特徴とするコンピュータプログラム。

[15] コンピュータ読み取り可能な記録媒体であって、請求項14に記載のコンピュータプログラムが記録されている

ことを特徴とする記録媒体。

[16] コンテンツの再生を行うコンテンツ再生装置に用いられる機器情報更新方法であって、

前記コンテンツ再生装置は、機器識別子と、模倣により製造された不正な機器を検出する不正機器検出装置により生成された検証値とを対応づけて記憶する記憶手段を備え、

前記機器情報更新方法は、

前記機器識別子と前記検証値とを、前記不正機器検出装置に通知する通知ステップと、

前記通知に対する応答として、前記不正機器検出装置により可搬媒体に書き込まれた、機器識別子と前記不正機器検出装置により生成された検証値とを、当該可搬媒体から取得する取得ステップと、

前記記憶手段に記憶されている前記機器識別子と取得した機器識別子とが一致する場合に、前記記憶手段に記憶されている検証値に替えて、取得した前記検証値と前記機器識別子とを対応づけて記憶させる更新ステップと

を含むことを特徴とする機器情報更新方法。

[17] コンテンツの再生を行うコンテンツ再生装置に用いられるコンピュータプログラムであって、

前記コンテンツ再生装置は、機器識別子と、模倣により製造された不正な機器を検出する不正機器検出装置により生成された検証値とを対応づけて記憶する記憶手段を備え、

前記コンピュータプログラムは、

前記機器識別子と前記検証値とを、前記不正機器検出装置に通知する通知ステッ

プと、

前記通知に対する応答として、前記不正機器検出装置により可搬媒体に書き込まれた、機器識別子と前記不正機器検出装置により生成された検証値とを、当該可搬媒体から取得する取得ステップと、

前記記憶手段に記憶されている前記機器識別子と取得した機器識別子とが一致する場合に、前記記憶手段に記憶されている検証値に替えて、取得した前記検証値と前記機器識別子とを対応づけて記憶させる更新ステップと

を含むことを特徴とするコンピュータプログラム。

[18] コンピュータ読み取り可能な記録媒体であって、請求項17に記載のコンピュータプログラムが記録されている

ことを特徴とする記録媒体。

[19] コンテンツの再生を行うコンテンツ再生装置に用いられる集積回路であって、

機器識別子と、模倣により製造された不正な機器を検出する不正機器検出装置により生成された検証値とを対応づけて記憶している記憶手段と、

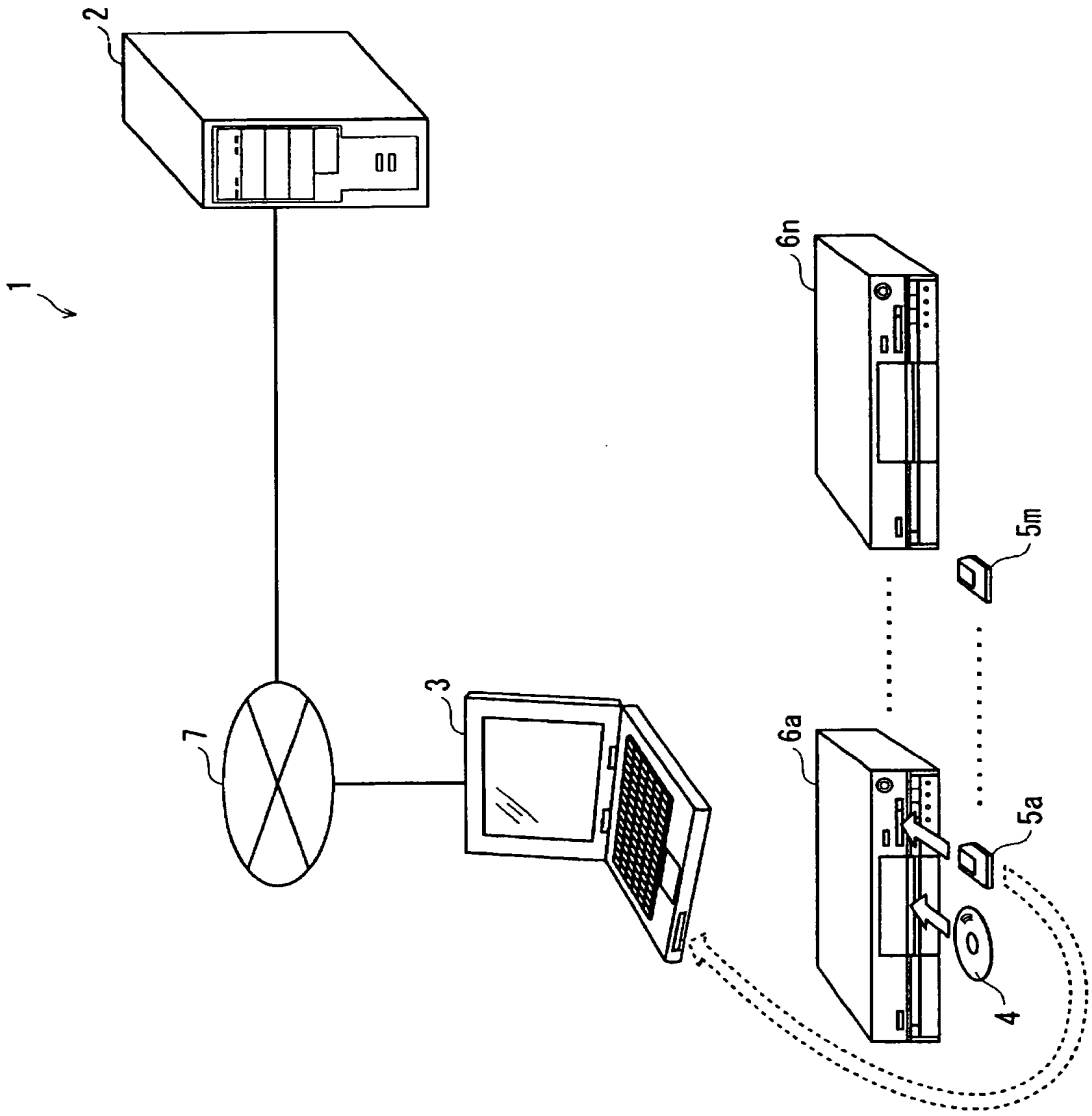
前記機器識別子と前記検証値とを、前記不正機器検出装置に通知する通知手段と、

前記通知に対する応答として、前記不正機器検出装置により可搬媒体に書き込まれた、機器識別子と前記不正機器検出装置により生成された検証値とを、当該可搬媒体から取得する取得手段と、

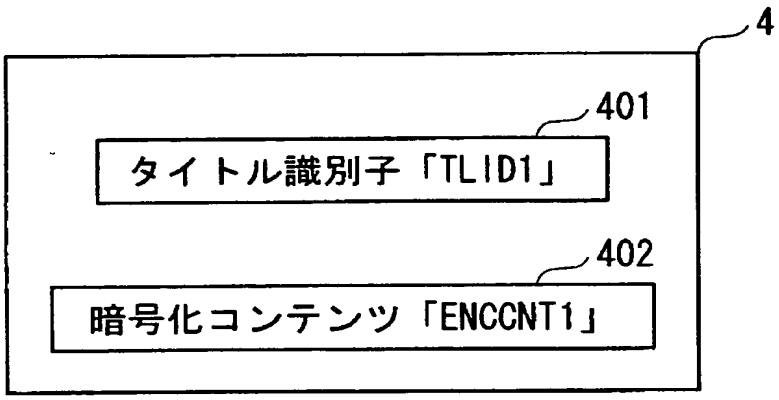
前記記憶手段に記憶されている前記機器識別子と取得した前記機器識別子とが一致する場合に、前記記憶手段に記憶されている検証値に替えて、取得した前記検証値と前記機器識別子とを対応づけて記憶させる更新手段と

を備えることを特徴とする集積回路。

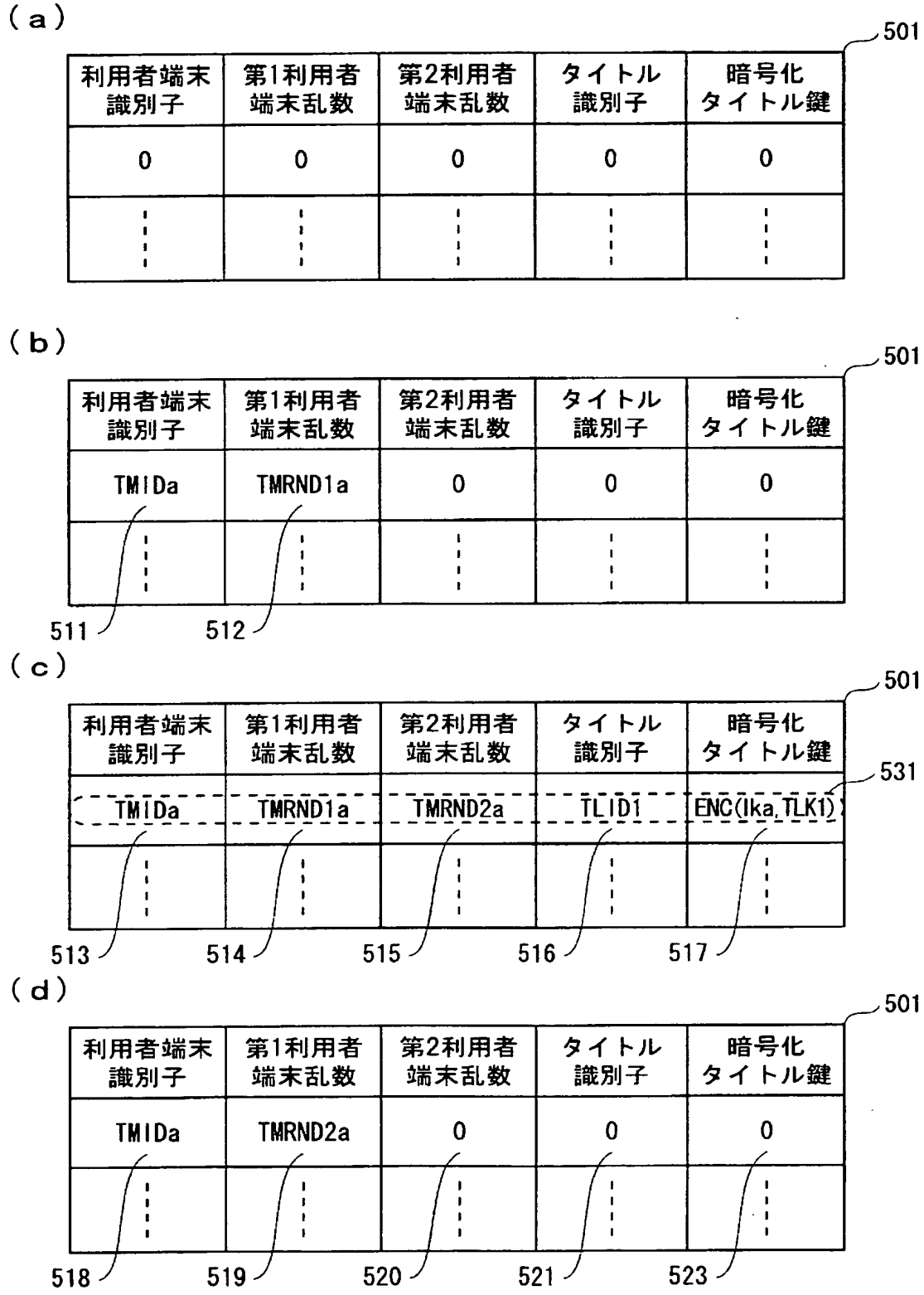
[図1]



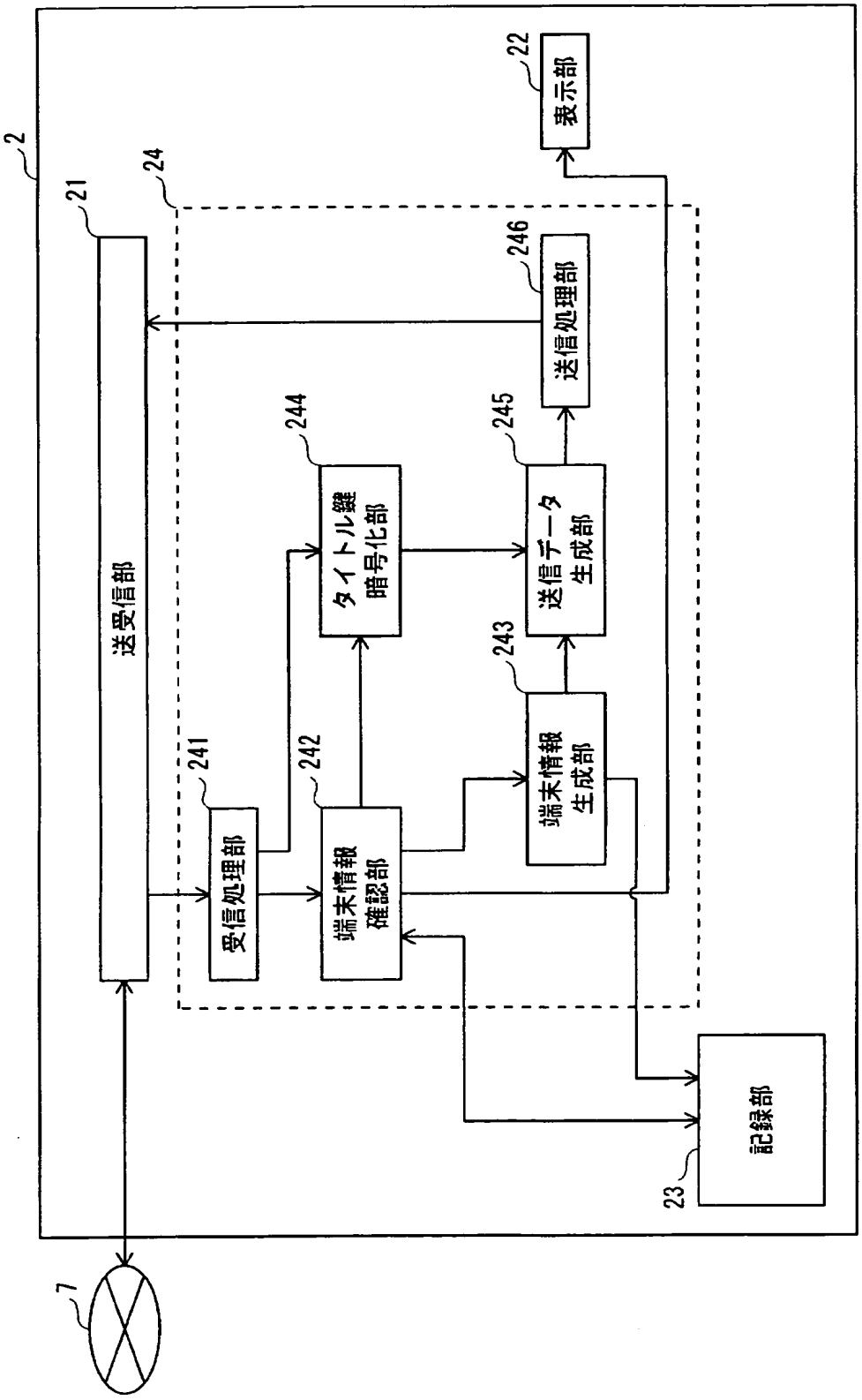
[図2]



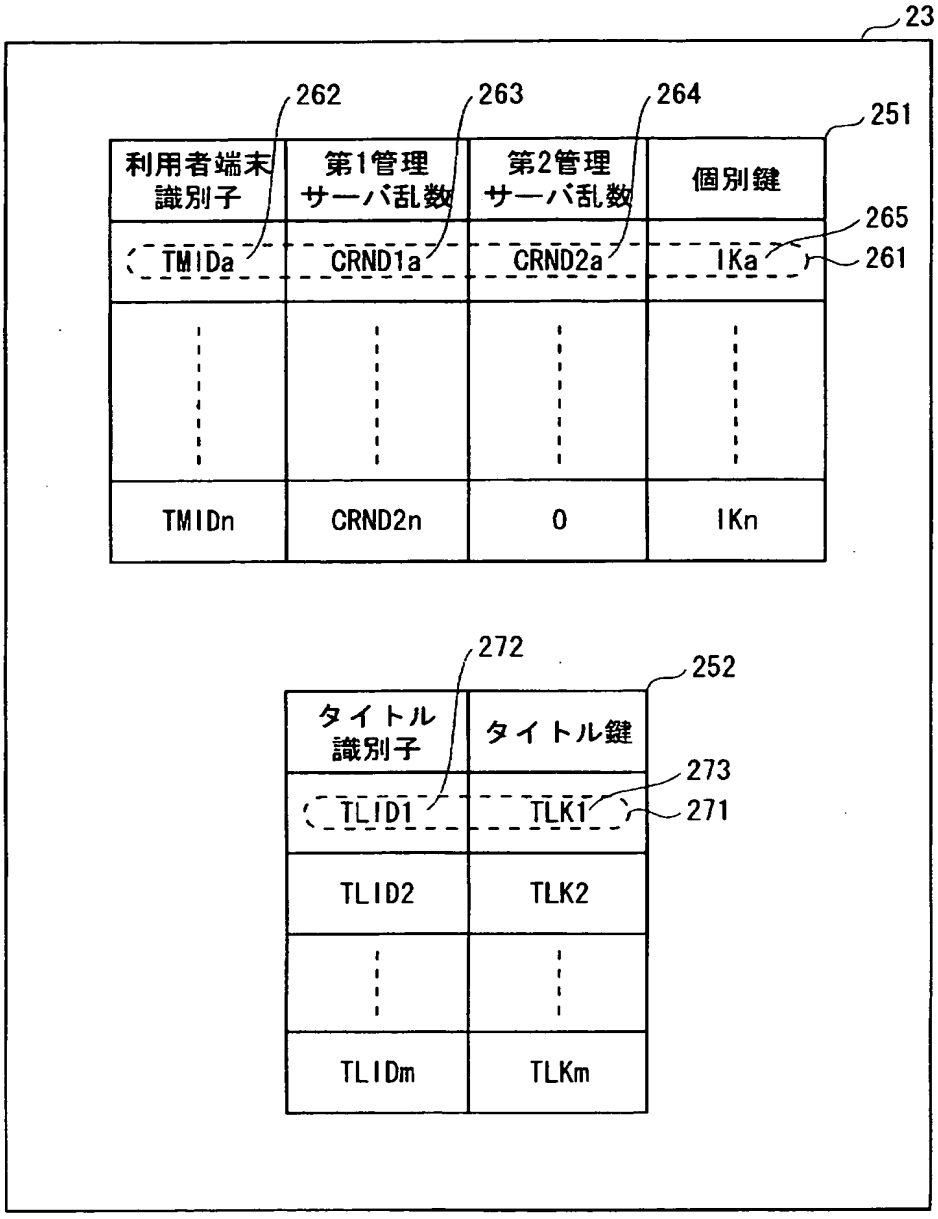
[図3]


(a)
501
利用者端末識別子
第1利用者端末乱数
第2利用者端末乱数
タイトル識別子
暗号化タイトル鍵
0
0
0
0
0
(b)
501
利用者端末識別子
第1利用者端末乱数
第2利用者端末乱数
タイトル識別子
暗号化タイトル鍵
TMIDa
TMRND1a
0
0
0
511
512
(c)
501
利用者端末識別子
第1利用者端末乱数
第2利用者端末乱数
タイトル識別子
暗号化タイトル鍵
531
TMIDa
TMRND1a
TMRND2a
TLID1
ENC(Ika,TLK1)
513
514
515
516
517
(d)
501
利用者端末識別子
第1利用者端末乱数
第2利用者端末乱数
タイトル識別子
暗号化タイトル鍵
TMIDa
TMRND2a
0
0
0
518
519
520
521
523

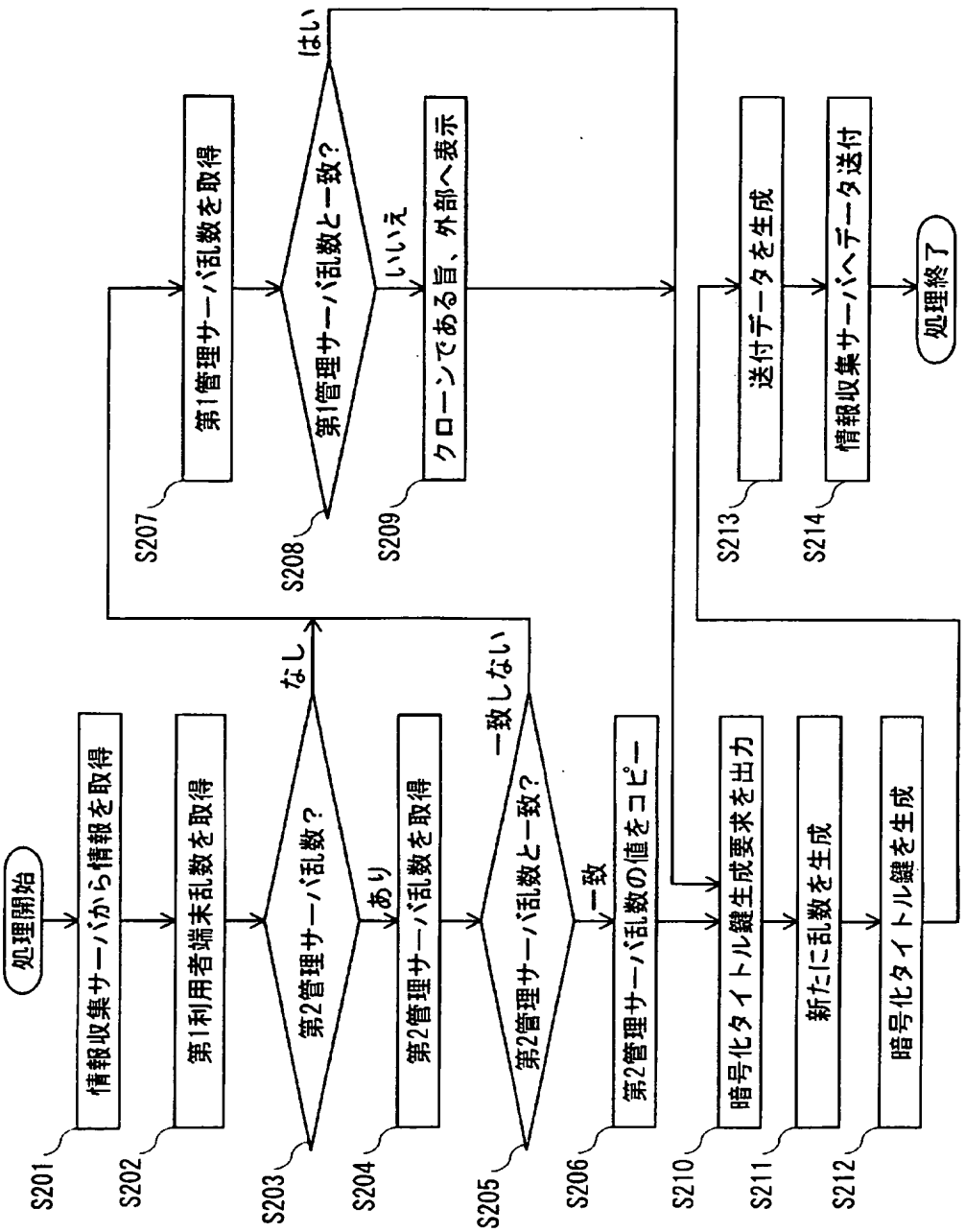
[図4]


2
21
送受信部
24
22
表示部
246
送信処理部
244
タイトル鍵
暗号化部
245
送信データ
生成部
243
端末情報
生成部
241
受信処理部
242
端末情報
確認部
23
記録部
7

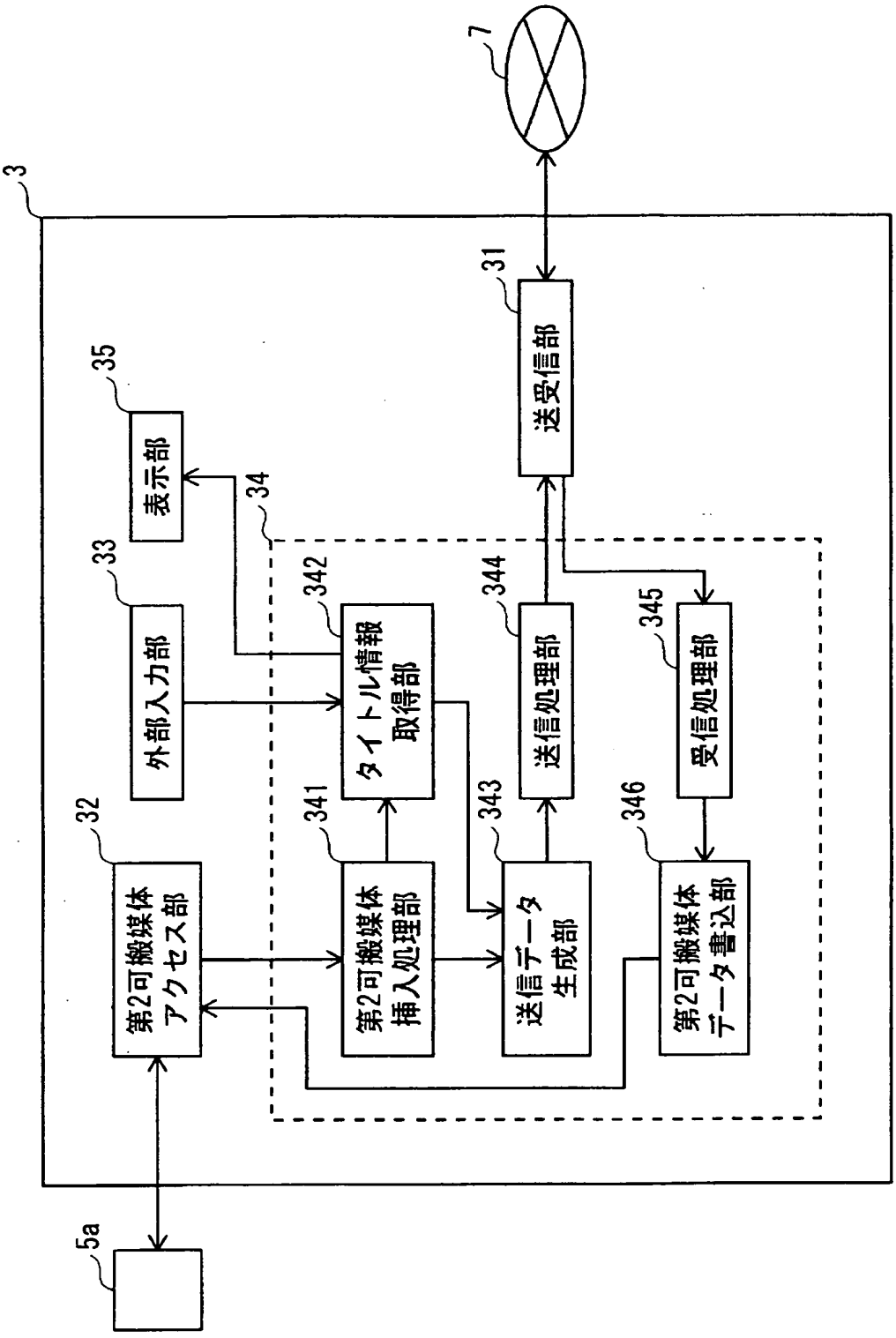
[図5]


23
262
263
264
251
利用者端末識別子
第1管理サーバ乱数
第2管理サーバ乱数
個別鍵
265
261
TMIDa
CRND1a
CRND2a
IKa
TMIDn
CRND2n
0
IKn
272
252
タイトル識別子
タイトル鍵
273
271
TLID1
TLK1
TLID2
TLK2
TLIDm
TLKm

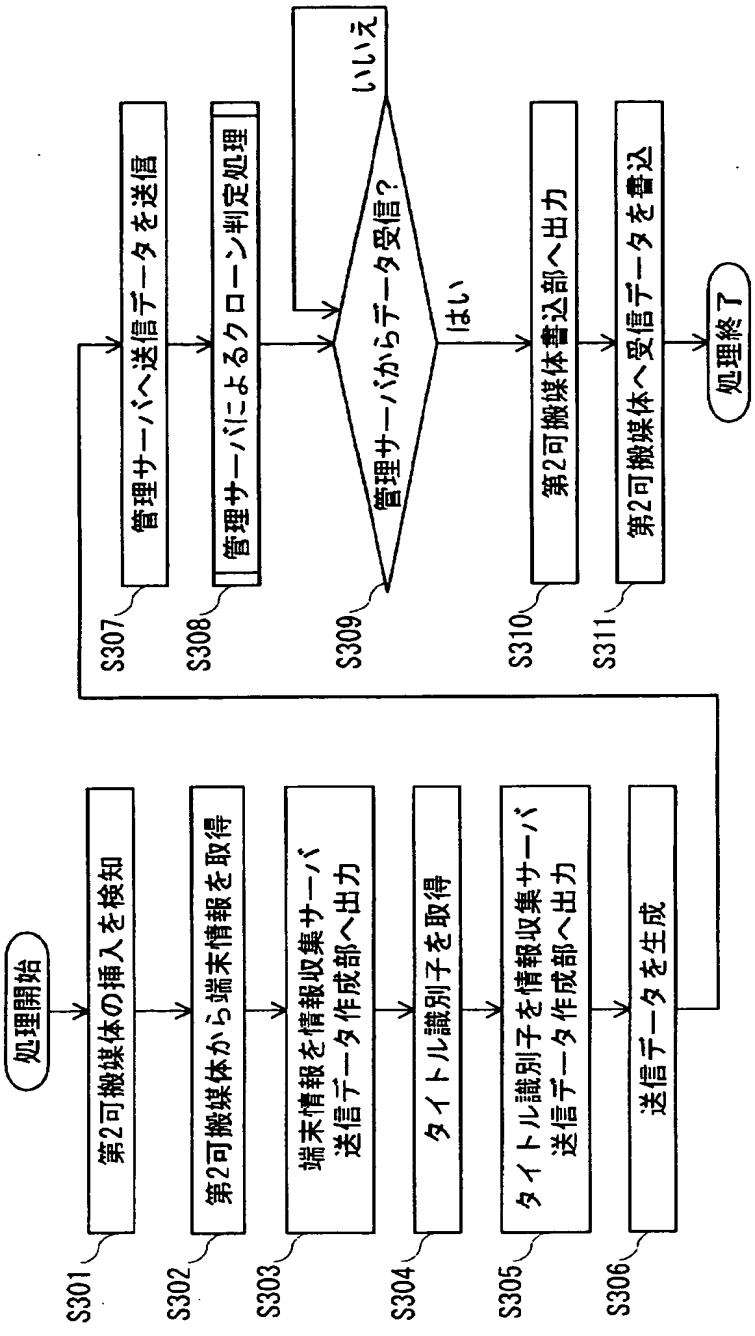
[図6]


処理開始
情報収集サーバから情報を取得
第1利用者端末乱数を取得
第2管理サーバ乱数？
なし
あり
第2管理サーバ乱数を取得
第2管理サーバ乱数と一致？
一致しない
一致
第2管理サーバ乱数の値をコピー
第1管理サーバ乱数を取得
第1管理サーバ乱数と一致？
はい
いいえ
クローンである旨、外部へ表示
暗号化タイトル鍵生成要求を出力
新たに乱数を生成
暗号化タイトル鍵を生成
送付データを生成
情報収集サーバへデータ送付
処理終了
S201
S202
S203
S204
S205
S206
S207
S208
S209
S210
S211
S212
S213
S214

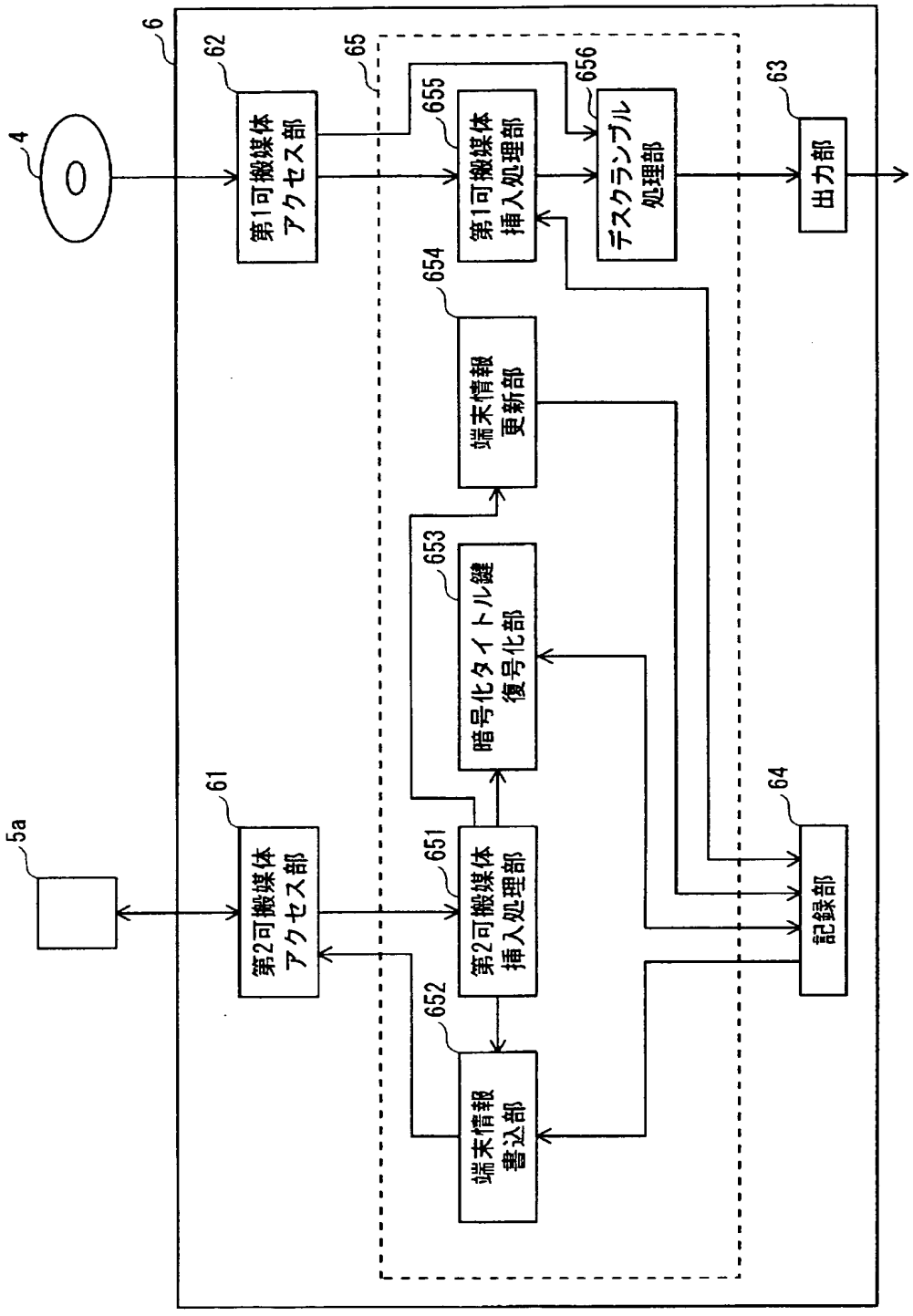
[図7]


7
3
31
送受信部
35
表示部
34
33
外部入力部
342
タイトル情報取得部
344
送信処理部
345
受信処理部
32
第2可搬媒体アクセス部
341
第2可搬媒体挿入処理部
343
送信データ生成部
346
第2可搬媒体データ書込部
5a

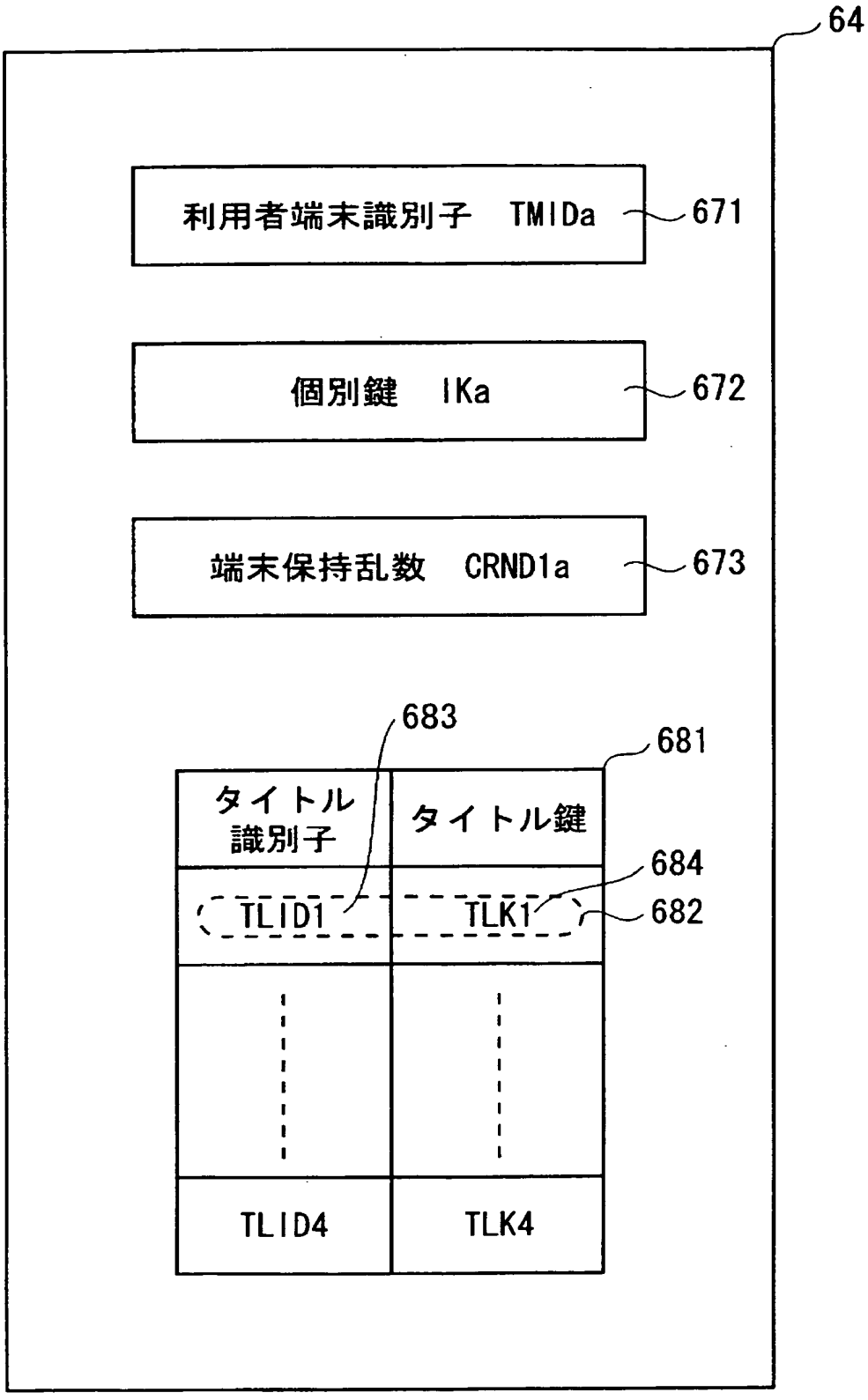
[図8]


処理開始
第2可搬媒体の挿入を検知
第2可搬媒体から端末情報を取得
端末情報を情報収集サーバ送信データ作成部へ出力
タイトル識別子を取得
タイトル識別子を情報収集サーバ送信データ作成部へ出力
送信データを生成
管理サーバへ送信データを送信
管理サーバによるクローン判定処理
管理サーバからデータ受信?
いいえ
はい
第2可搬媒体書込部へ出力
第2可搬媒体へ受信データを書込
処理終了
S301
S302
S303
S304
S305
S306
S307
S308
S309
S310
S311

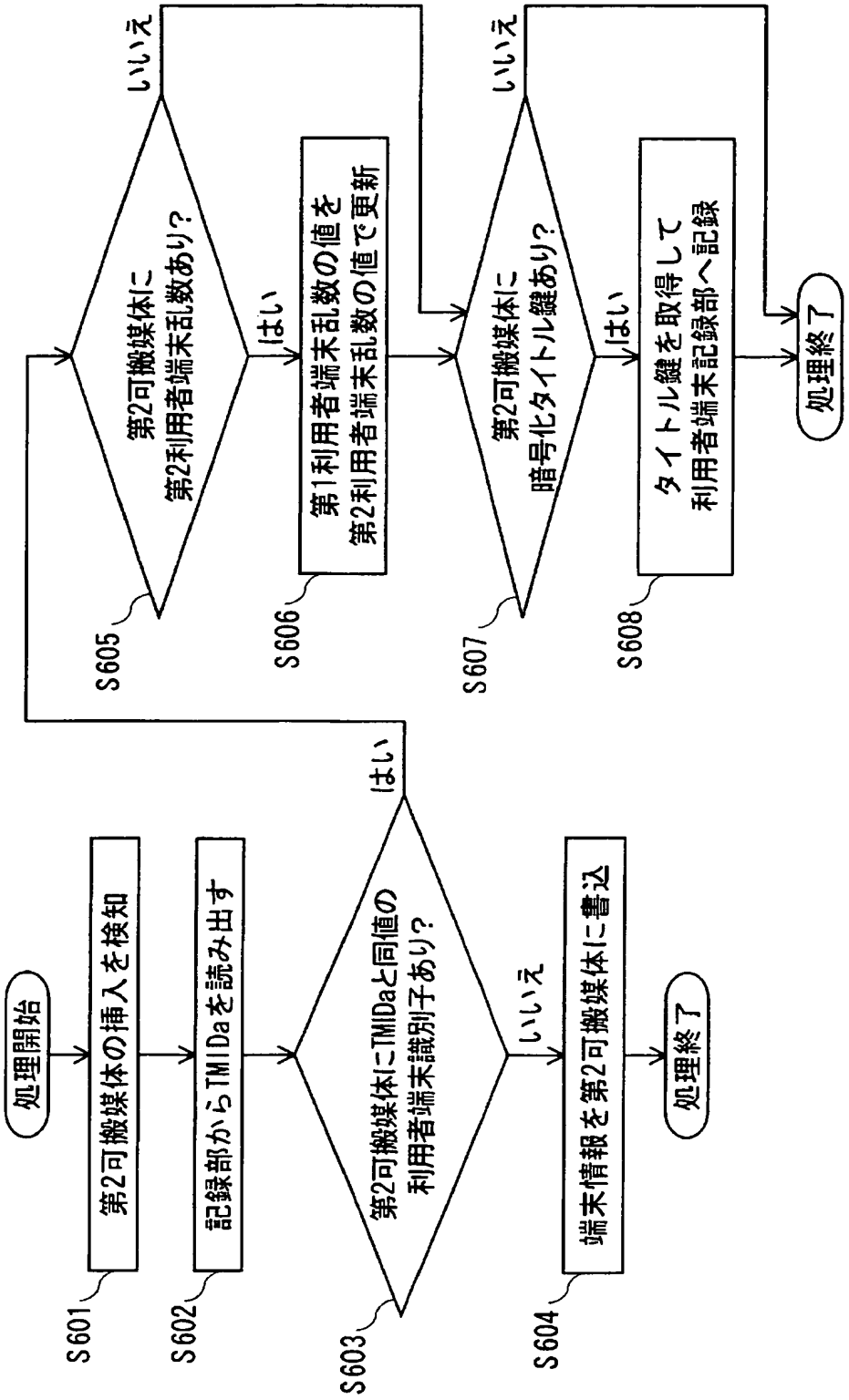
[図9]


6
62
65
655
656
63
4
第1可搬媒体
アクセス部
第1可搬媒体
挿入処理部
デスクランブル
処理部
出力部
654
端末情報
更新部
653
暗号化タイトル鍵
復号化部
5a
61
651
64
第2可搬媒体
アクセス部
第2可搬媒体
挿入処理部
記録部
652
端末情報
書込部

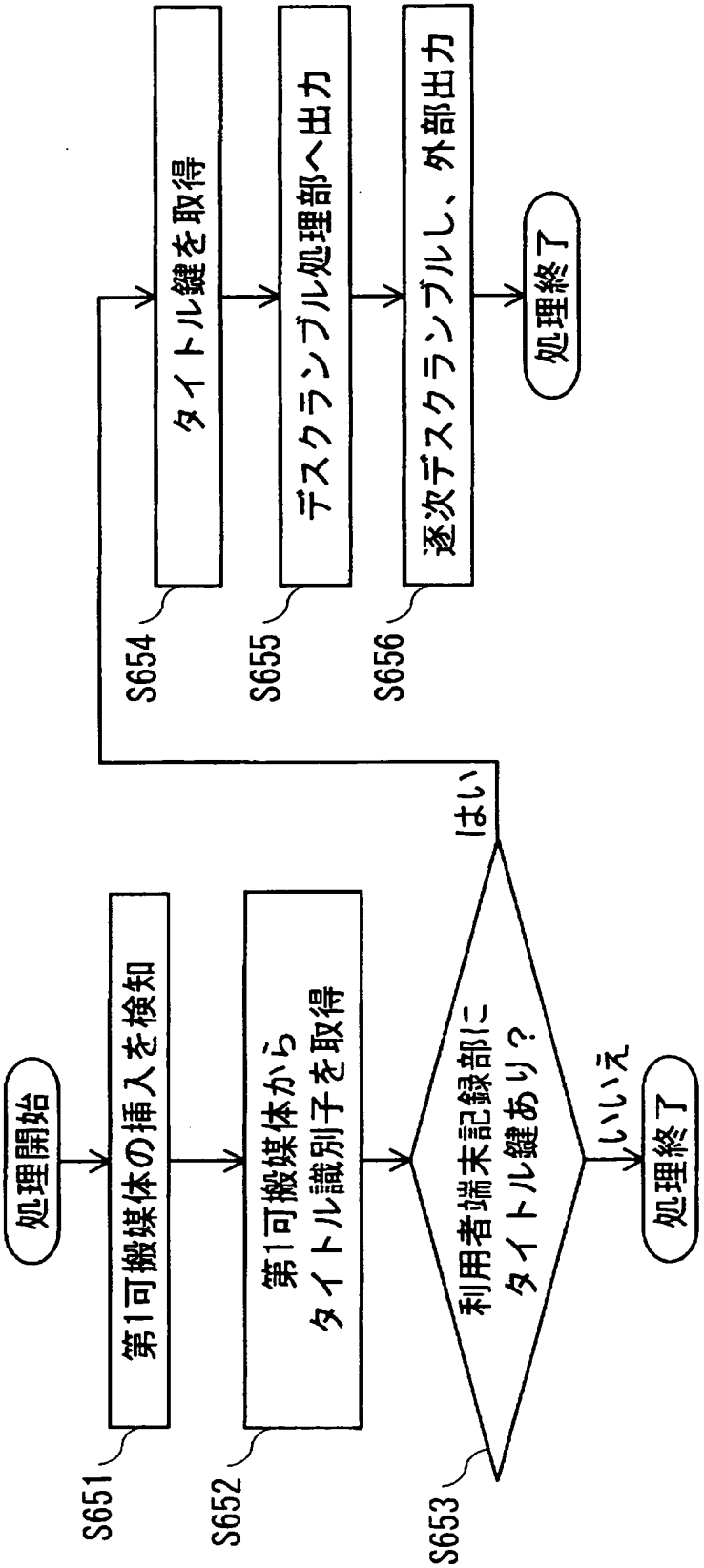
[図10]


64
利用者端末識別子 TMIDa
671
個別鍵 IKa
672
端末保持乱数 CRND1a
673
683
681
タイトル識別子
タイトル鍵
684
TLID1
TLK1
682
TLID4
TLK4

[図11]


処理開始
第2可搬媒体の挿入を検知
S601
記録部からTMIDaを読み出す
S602
第2可搬媒体にTMIDaと同値の利用者端末識別子あり?
S603
はい
いいえ
端末情報を第2可搬媒体に書込
S604
処理終了
第2可搬媒体に第2利用者端末乱数あり?
S605
いいえ
はい
第1利用者端末乱数の値を第2利用者端末乱数の値で更新
S606
第2可搬媒体に暗号化タイトル鍵あり?
S607
いいえ
はい
タイトル鍵を取得して利用者端末記録部へ記録
S608
処理終了

[図12]


処理開始
第1可搬媒体の挿入を検知
S651
第1可搬媒体から
タイトル識別子を取得
S652
利用者端末記録部に
タイトル鍵あり？
S653
はい
いいえ
タイトル鍵を取得
S654
デスクランブル処理部へ出力
S655
逐次デスクランブルし、外部出力
S656
処理終了
処理終了

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２００５／０２２７８８

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl. *G06F21/20(2006.01), G06F21/24(2006.01), H04L9/08(2006.01), H04N7/16(2006.01), H04N7/167(2006.01)*

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl. *G06F21/20(2006.01), G06F21/24(2006.01), H04L9/08(2006.01), H04N7/16(2006.01), H04N7/167(2006.01)*

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００６年
日本国実用新案登録公報	１９９６－２００６年
日本国登録実用新案公報	１９９４－２００６年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2000-222534 A（株式会社日立製作所）2000.08.11, 特許請求の範囲、明細書第0042段落及び同第0043段落（ファミリーなし）	9
Y	同上	1, 2, 5-8, 10-19
A	同上	3, 4
Y	JP 2001-166996 A（松下電器産業株式会社）2001.06.22, 図面図２ & US 6850914 B1 & US 6581160 B1 & EP 1098311 A1	1, 2, 5-8, 10-19
A	同上	3, 4

☑ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 １４．０３．２００６	国際調査報告の発送日 ２８．０３．２００６
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　９５５５ 宮司　卓佳 電話番号　０３－３５８１－１１０１　内線　３５４６

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００５年４月）

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２００５／０２２７８８

C（続き）. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	WO 2004/023524 A2 (MATSUSHITA ELECTRIC INDUSTRIAL Co., LTD.) 2004.03.18, 全文, 全図 & US 2004/0049464 A1	1-19
A	WO 2003/034651 A1 (松下電器産業株式会社) 2003.04.24, 図面図２及び図１５ & US 2004/0260923 A1 & EP 1445888 A1	3, 4